Cisco Security Appliance Command Reference

For the Cisco ASA 5500 Series and Cisco PIX 500 Series

Software Version 8.0(5)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12173-02

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Cisco Security Appliance Command Reference
Copyright © 2009 Cisco Systems, Inc. All rights reserved.

About This Guide

This preface introduces the *Cisco Security Appliance Command Reference*.

This preface includes the following sections:

- Document Objectives, page 3
- Audience, page 4
- Document Organization, page 4
- Document Conventions, page 4
- Related Documentation, page 5
- Obtaining Documentation and Submitting a Service Request, page 5

Document Objectives

This guide contains the commands available for use with the security appliance to protect your network from unauthorized use and to establish Virtual Private Networks to connect remote sites and users to your network.

You can also configure and monitor the security appliance by using ASDM, a web-based GUI application. ASDM includes configuration wizards to guide you through some common configuration scenarios, and online Help for less common scenarios. For more information, see: http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm.

This guide applies to the Cisco PIX 500 series security appliances (PIX 515/515E, PIX 525, and PIX 535) and the Cisco ASA 5500 series security appliances (ASA 5505, ASA 5510, ASA 5520, ASA 5540, and ASA 5550). Throughout this guide, the term “security appliance” applies generically to all supported models, unless specified otherwise. The PIX 501, PIX 506E, and PIX 520 security appliances are not supported in software Version 8.0.

Audience

This guide is for network managers who perform any of the following tasks:

- Manage network security
- Install and configure firewall/security appliances
- Configure VPNs
- Configure intrusion detection software

Use this guide with the *Cisco Security Appliance Command Line Configuration Guide*.

Document Organization

- "Using the Command-Line Interface" introduces you to the security appliance commands and access modes.
- Chapters 1 through 32 list all commands in alphabetical order.

Document Conventions

The security appliance command syntax descriptions use the following conventions:

Command descriptions use these conventions:

- Braces ({ }) indicate a required choice.
- Square brackets ([ ]) indicate optional elements.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- **Boldface** indicates commands and keywords that are entered literally as shown.
- *Italics* indicate arguments for which you supply values.

Examples use these conventions:

- Examples depict screen displays and the command line in `screen` font.
- Information you need to enter in examples is shown in **`boldface screen`** font.
- Variables for which you must supply a value are shown in *`italic screen`* font.
- Examples might include output from different platforms; for example, you might not recognize an interface type in an example because it is not available on your platform. Differences should be minor.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

For information on modes, prompts, and syntax, see Chapter , "Using the Command-Line Interface."

Related Documentation

For more information, see the following documentation:

- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Release Notes for Cisco ASDM*
- *Cisco ASA 5580 Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Hardware Maintenance Guide*
- *Cisco ASA 5500 Getting Started Guide*
- *Cisco ASA 5505 Getting Started Guide*
- *Cisco PIX Security Appliance Release Notes*
- *Cisco PIX 515E Quick Start Guide*
- *Cisco Security Appliance System Log Messages*
- *Cisco ASA 5580 Adaptive Security Appliance System Log Messages Guide*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Release Notes for Cisco Secure Desktop*
- *Migration Guide for Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations*
- *Migrating to ASA for VPN 3000 Concentrator Series Administrators*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Using the Command-Line Interface

This chapter describes how to use the CLI on the security appliance and includes the following topics:

- Firewall Mode and Security Context Mode, page 7
- Command Modes and Prompts, page 8
- Syntax Formatting, page 9
- Abbreviating Commands, page 9
- Command-Line Editing, page 9
- Command Completion, page 9
- Command Help, page 10
- Filtering show Command Output, page 10
- Command Output Paging, page 12
- Adding Comments, page 12
- Text Configuration Files, page 12

Note The CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the security appliance operating system is not a version of Cisco IOS software. Do not assume that a Cisco IOS CLI command works with or has the same function on the security appliance.

Firewall Mode and Security Context Mode

The security appliance runs in a combination of the following modes:

- Transparent firewall or routed firewall mode

  The firewall mode determines if the security appliance runs as a Layer 2 or Layer 3 firewall.

- Multiple context or single context mode

  The security context mode determines if the security appliance runs as a single device or as multiple security contexts, which act like virtual devices.

Some commands are only available in certain modes.

Command Modes and Prompts

The security appliance CLI includes command modes. Some commands can only be entered in certain modes. For example, to enter commands that show sensitive information, you need to enter a password and enter a more privileged mode. Then, to ensure that configuration changes are not entered accidentally, you have to enter a configuration mode. All lower commands can be entered in higher modes, for example, you can enter a privileged EXEC command in global configuration mode.

When you are in the system configuration or in single context mode, the prompt begins with the hostname:

```
hostname
```

When you are within a context, the prompt begins with the hostname followed by the context name:

```
hostname/context
```

The prompt changes depending on the access mode:

- User EXEC mode

  User EXEC mode lets you see minimum security appliance settings. The user EXEC mode prompt appears as follows when you first access the security appliance:

  ```
  hostname>
  ```

  ```
  hostname/context>
  ```

- Privileged EXEC mode

  Privileged EXEC mode lets you see all current settings up to your privilege level. Any user EXEC mode command will work in privileged EXEC mode. Enter the **enable** command in user EXEC mode, which requires a password, to start privileged EXEC mode. The prompt includes the number sign (#):

  ```
  hostname#
  ```

  ```
  hostname/context#
  ```

- Global configuration mode

  Global configuration mode lets you change the security appliance configuration. All user EXEC, privileged EXEC, and global configuration commands are available in this mode. Enter the **configure terminal** command in privileged EXEC mode to start global configuration mode. The prompt changes to the following:

  ```
  hostname(config)#
  ```

  ```
  hostname/context(config)#
  ```

- Command-specific configuration modes

  From global configuration mode, some commands enter a command-specific configuration mode. All user EXEC, privileged EXEC, global configuration, and command-specific configuration commands are available in this mode. For example, the **interface** command enters interface configuration mode. The prompt changes to the following:

  ```
  hostname(config-if)#
  ```

  ```
  hostname/context(config-if)#
  ```

Syntax Formatting

Command syntax descriptions use the following conventions:

Table 1 Syntax Conventions

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
|	A vertical bar indicates a choice within an optional or required set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Abbreviating Commands

You can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter `wr t` to view the configuration instead of entering the full command `write terminal`, or you can enter `en` to start privileged mode and `conf t` to start configuration mode. In addition, you can enter `0` to represent `0.0.0.0`.

Command-Line Editing

The security appliance uses the same command-line editing conventions as Cisco IOS software. You can view all previously entered commands with the **show history** command or individually with the up arrow or **^p** command. Once you have examined a previously entered command, you can move forward in the list with the down arrow or **^n** command. When you reach a command you wish to reuse, you can edit it or press the **Enter** key to start it. You can also delete the word to the left of the cursor with **^w**, or erase the line with **^u**.

The security appliance permits up to 512 characters in a command; additional characters are ignored.

Command Completion

To complete a command or keyword after entering a partial string, press the **Tab** key. The security appliance only completes the command or keyword if the partial string matches only one command or keyword. For example, if you enter **s** and press the **Tab** key, the security appliance does not complete the command because it matches more than one command. However, if you enter **dis**, the **Tab** key completes the command **disable**.

Command Help

Help information is available from the command line by entering the following commands:

- **help** *command_name*

  Shows help for the specific command.

- **help ?**

  Shows commands for which there is help.

- *command_name* **?**

  Shows a list of arguments available.

- *string***?** (no space)

  Lists the possible commands that start with the string.

- **?** and **+?**

  Lists all commands available. If you enter **?**, the security appliance shows only commands available for the current mode. To show all commands available, including those for lower modes, enter **+?**.

Note If you want to include a question mark (?) in a command string, you must press **Ctrl-V** before typing the question mark so you do not inadvertently invoke CLI help.

Filtering show Command Output

You can use the vertical bar (|) with any **show** command and include a filter option and filtering expression. The filtering is performed by matching each output line with a regular expression, similar to Cisco IOS software. By selecting different filter options you can include or exclude all output that matches the expression. You can also display all output beginning with the line that matches the expression.

The syntax for using filtering options with the **show** command is as follows:

```
hostname# show command | {include | exclude | begin | grep [-v]} regexp
```

In this command string, the first vertical bar (|) is the operator and must be included in the command. This operator directs the output of the **show** command to the filter. In the syntax diagram, the other vertical bars (|) indicate alternative options and are not part of the command.

The **include** option includes all output lines that match the regular expression. The **grep** option without **-v** has the same effect. The **exclude** option excludes all output lines that match the regular expression. The **grep** option with **-v** has the same effect. The **begin** option shows all the output lines starting with the line that matches the regular expression.

Replace *regexp* with any Cisco IOS regular expression. The regular expression is not enclosed in quotes or double-quotes, so be careful with trailing white spaces, which will be taken as part of the regular expression.

When creating regular expressions, you can use any letter or number that you want to match. In addition, certain keyboard characters called *metacharacters* have special meaning when used in regular expressions.

Use **Ctrl+V** to escape all of the special characters in the CLI, such as question mark (?) or a tab. For example, type **d[Ctrl+V]?g** to enter **d?g** in the configuration.

Table 1-2 lists the metacharacters that have special meanings.

Table 1-2 regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp***)**	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*****	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x***}** or **{***x***,}**	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc***]**	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc***]**	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a-c***]**	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **" test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.

Table 1-2 regex Metacharacters (continued)

Character	Description	Notes
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Command Output Paging

On commands such as **help** or**?**, **show**, **show xlate**, or other commands that provide long listings, you can determine if the information displays a screen and pauses, or lets the command run to completion. The **pager** command lets you choose the number of lines to display before the More prompt appears.

When paging is enabled, the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX **more** command:

- To view another screen, press the Space bar.
- To view the next line, press the **Enter** key.
- To return to the command line, press the **q** key.

Adding Comments

You can precede a line with a colon (:) to create a comment. However, the comment only appears in the command history buffer and not in the configuration. Therefore, you can view the comment with the **show history** command or by pressing an arrow key to retrieve a previous command, but because the comment is not in the configuration, the **write terminal** command does not display it.

Text Configuration Files

This section describes how to format a text configuration file that you can download to the security appliance, and includes the following topics:

- How Commands Correspond with Lines in the Text File, page 13

- Command-Specific Configuration Mode Commands, page 13
- Automatic Text Entries, page 13
- Line Order, page 13
- Commands Not Included in the Text Configuration, page 14
- Passwords, page 14
- Multiple Security Context Files, page 14

How Commands Correspond with Lines in the Text File

The text configuration file includes lines that correspond with the commands described in this guide.

In examples, commands are preceded by a CLI prompt. The prompt in the following example is "hostname(config)#":

```
hostname(config)# context a
```

In the text configuration file you are not prompted to enter commands, so the prompt is omitted:

```
context a
```

Command-Specific Configuration Mode Commands

Command-specific configuration mode commands appear indented under the main command when entered at the command line. Your text file lines do not need to be indented, as long as the commands appear directly following the main command. For example, the following unindented text is read the same as indented text:

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

Automatic Text Entries

When you download a configuration to the security appliance, the security appliance inserts some lines automatically. For example, the security appliance inserts lines for default settings or for the time the configuration was modified. You do not need to enter these automatic entries when you create your text file.

Line Order

For the most part, commands can be in any order in the file. However, some lines, such as ACEs, are processed in the order they appear, and the order can affect the function of the access list. Other commands might also have order requirements. For example, you must enter the **nameif** command for an interface first because many subsequent commands use the name of the interface. Also, commands in a command-specific configuration mode must directly follow the main command.

Commands Not Included in the Text Configuration

Some commands do not insert lines in the configuration. For example, a runtime command such as **show running-config** does not have a corresponding line in the text file.

Passwords

The login, enable, and user passwords are automatically encrypted before they are stored in the configuration. For example, the encrypted form of the password “cisco” might look like jMorNbK0514fadBh. You can copy the configuration passwords to another security appliance in their encrypted form, but you cannot unencrypt the passwords yourself.

If you enter an unencrypted password in a text file, the security appliance does not automatically encrypt them when you copy the configuration to the security appliance. The security appliance only encrypts them when you save the running configuration from the command line using the **copy running-config startup-config** or **write memory** command.

Multiple Security Context Files

For multiple security contexts, the entire configuration consists of multiple parts:

- The security context configurations
- The system configuration, which identifies basic settings for the security appliance, including a list of contexts
- The admin context, which provides network interfaces for the system configuration

  The system configuration does not include any interfaces or network settings for itself. Rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses a context that is designated as the admin context.

Each context is similar to a single context mode configuration. The system configuration differs from a context configuration in that the system configuration includes system-only commands (such as a list of all contexts) while other typical commands are not present (such as many interface parameters).

CHAPTER 2

aaa accounting through accounting-server-group Commands

aaa accounting command

To send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI, use the **aaa accounting command** command in global configuration mode. To disable support for command accounting, use the **no** form of this command.

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

Syntax Description

tacacs+-server-tag	Specifies the server or group of TACACS+ servers to which accounting records are sent, as specified by the **aaa-server protocol** command.
privilege *level*	If you customize the command privilege level using the **privilege** command, you can limit which commands the security appliance accounts for by specifying a minimum privilege level. The security appliance does not account for commands that are below the minimum privilege level.

Defaults

The default privilege level is 0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you configure the **aaa accounting command** command, each command other than **show** commands entered by an administrator is recorded and sent to the accounting server or servers.

Examples

The following example specifies that accounting records will be generated for any supported command, and that these records are sent to the server from the group named adminserver.

```
hostname(config)# aaa accounting command adminserver
```

Related Commands

Command	Description
aaa accounting	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command).
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa accounting console

To enable support for AAA accounting for administrative access, use the **aaa accounting console** command in global configuration mode. To disable support for aaa accounting for administrative access, use the **no** form of this command.

aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

no aaa accounting {**serial | telnet | ssh | enable**} **console** *server-tag*

Syntax Description

enable	Enables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
serial	Enables the generation of accounting records to mark the establishment and termination of admin sessions that are established via the serial console interface.
server-tag	Specifies the server group to which accounting records are sent, defined by the **aaa-server protocol** command. Valid server group protocols are RADIUS and TACACS+.
ssh	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over Telnet.

Defaults

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must specify the name of the server group, previously specified in an **aaa-server** command.

Examples

The following example specifies that accounting records will be generated for enable access, and that these records are sent to the server named adminserver.

```
hostname(config)# aaa accounting enable console adminserver
```

Related Commands

Command	Description
aaa accounting match	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command),
aaa accounting command	Specifies that each command, or commands of a specified privilege level or higher, entered by an administrator/user is recorded and sent to the accounting server or servers.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa accounting include, exclude

To enable accounting for TCP or UDP connections through the security appliance, use the **aaa accounting include** command in global configuration mode. To exclude addresses from accounting, use the **aaa accounting exclude** command. To disable accounting, use the **no** form of this command.

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from accounting if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require accounting. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require accounting.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server host** command.
service	Specifies the services that require accounting. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port* • **udp**/*port*

Defaults

By default, AAA accounting for administrative access is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

To enable accounting for traffic that is specified by an access list, use the **aaa accounting match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa accounting include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa accounting match** command.

Examples

The following example enables accounting on all TCP connections:

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

Related Commands

Command	Description
aaa accounting match	Enables accounting for traffic specified by an access list.
aaa accounting command	Enables accounting of administrative access.
aaa-server host	Configures the AAA server.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa accounting match

To enable accounting for TCP and UDP connections through the security appliance, use the **aaa accounting match** command in global configuration mode. To disable accounting for traffic, use the **no** form of this command.

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies the traffic that requires accounting my matching an **access-list** name. Permit entries in the access list are accounted, while deny entries are exempt from accounting. This command is only supported for TCP and UDP traffic. A warning message is displayed if you enter this command and it references an access list that permits other protocols.
interface_name	Specifies the interface name from which users require accounting.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting using the **accounting-mode** command in aaa-server protocol configuration mode.

You cannot use the **aaa accounting match** command in the same configuration as the **aaa accounting include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

Examples

The following example enables accounting for traffic matching a specific access list acl2:

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

Related Commands

Command	Description
aaa accounting include, exclude	Enables accounting by specifying the IP addresses directly in the command.
access-list extended	Creates an access list.
clear configure aaa	Removes AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication console

To authenticate users who access the security appliance CLI over a serial, SSH, HTTPS (ASDM), or Telnet connection, or to authenticate users who access privileged EXEC mode using the **enable** command, use the **aaa authentication console** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication {**serial | enable** | **telnet** | **ssh** | **http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**serial | enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

Syntax Description

enable	Authenticates users who access privileged EXEC mode when they use the **enable** command.
http	Authenticates ASDM users who access the security appliance over HTTPS. You only need to configure HTTPS authentication if you want to use a RADIUS or TACACS+ server. By default, ASDM uses the local database for authentication even if you do not configure this command.

LOCAL	Uses the local database for authentication. **LOCAL** is case sensitive. If the local database is empty, the following warning message appears:
	`Warning:local database is empty! Use 'username' command to define local users.`
	If the local database becomes empty when **LOCAL** is still present in the configuration, the following warning message appears:
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server-tag [**LOCAL**]	Specifies the AAA server group tag defined by the **aaa-server** command. HTTPS management authentication does not support the SDI protocol for a AAA server group. If you use the **LOCAL** keyword in addition to the *server-tag*, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. **LOCAL** is case sensitive. We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used.
serial	Authenticates users who access the security appliance using the serial Console port.
ssh	Authenticates users who access the security appliance using SSH.
telnet	Authenticates users who access the security appliance using Telnet.

Defaults

By default, fallback to the local database is disabled.

If the **aaa authentication telnet console** command is not defined, you can gain access to the security appliance CLI with the security appliance login password (set with the **password** command).

If the **aaa authentication http console** command is not defined, you can gain access to the security appliance (via ASDM) with no username and the security appliance enable password (set with the **enable password** command). If the **aaa** commands are defined, but the HTTPS authentication requests a time out, which implies the AAA servers might be down or not available, you can gain access to the security appliance using the default administrator username and the enable password. By default, the enable password is not set.

If the **aaa authentication ssh console** command is not defined, you can gain access to the security appliance CLI with the username **pix** and with the security appliance enable password (set with the **enable password** command). By default, the enable password is blank. This behavior differs from when you log into the security appliance without AAA configured; in that case, you use the login password (set by the **password** command).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before the security appliance can authenticate a Telnet or SSH user, you must first configure access to the security appliance using the **telnet** or **ssh** commands. These commands identify the IP addresses that are allowed to communicate with the security appliance.

Logging in to the Security Appliance

After you connect to the security appliance, you log in and access user EXEC mode.

- If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password (set with the **password** command). For SSH, you enter “pix” as the username, and enter the login password.
- If you enable Telnet or SSH authenticationusing this command, you enter the username and password as defined on the AAA server or local user database.

Accessing Privileged EXEC Mode

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

- If you do not configure enable authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use enable authentication.
- If you configure enable authentication, the security appliance prompts you for your username and password.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.

Accessing ASDM

By default, you can log into ASDM with a blank username and the enable password set by the **enable password** command. However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

Although you can configure HTTPS authentication using this command and specify the local database, that functionality is always enabled by default. You should only configure HTTPS authentication if you want to use a AAA server for authentication. HTTPS authentication does not support the SDI protocol for a AAA server group. The maximum username prompt for HTTPS authentication is 30 characters. The maximum password length is 16 characters.

No Support in the System Execution Space for AAA Commands

In multiple context mode, you cannot configure any AAA commands in the system configuration.

Number of Login Attempts Allowed

As the following table shows, the action of the prompts for authenticated access to the security appliance CLI differ, depending on the option you choose with the **aaa authentication console** command.

Option	Number of Login Attempts Allowed
enable	3 tries before access is denied
serial	Continual until success
ssh	3 tries before access is denied
telnet	Continual until success
http	Continual until success

Limiting User CLI and ASDM Access

You can configure management authorization with the **aaa authorization exec authentication-server** command to limit a local user, RADIUS, TACACS+, or LDAP user (if you map LDAP attributes to RADIUS attributes) from accessing the CLI, ASDM, or the **enable** command.

Note Serial access is not included in management authorization, so if you configure **aaa authentication serial console**, then any user who authenticates can access the console port.

To configure the user for management authorization, see the following requirements for each AAA server type or local user:

- RADIUS or LDAP (mapped) users—Configure the Service-Type attribute for one of the following values. (To map LDAP attributes, see the **ldap attribute-map** command.)
  - Service-Type 6 (Administrative)—Allows full access to any services specified by the **aaa authentication console** commands.
  - Service-Type 7 (NAS prompt)—Allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh**} **console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.

  - Service-Type 5 (Outbound)—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPSec and SSL) users can still authenticate and terminate their remote access sessions.

- TACACS+ users—Authorization is requested with the "service=shell" and the server responds with PASS or FAIL.
  - PASS, privilege level 1—Allows full access to any services specified by the **aaa authentication console** commands.
  - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh**} **console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - FAIL—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).
- Local users—Set the **service-type** command. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

Examples

The following example shows use of the **aaa authentication console** command for a Telnet connection to a RADIUS server with the server tag "radius":

```
hostname(config)# aaa authentication telnet console radius
```

The following example identifies the server group "AuthIn" for enable authentication.

```
hostname(config)# aaa authentication enable console AuthIn
```

The following example shows use of the **aaa authentication console** command with fallback to the LOCAL user database if all the servers in the group "svrgrp1" fail:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication	Enables or disables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Remove/reset the configured AAA accounting values.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the security appliance can understand.
service-type	Limits a local user CLI access.
show running-config aaa	Display the AAA configuration.

aaa authentication include, exclude

To enable authentication for connections through the security appliance, use the **aaa authentication include** command in global configuration mode. To exclude addresses from authentication, use the **aaa authentication exclude** command. To disable authentication, use the **no** form of this command.

aaa authentication {include | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

Syntax Description

exclude	Excludes the specified service and address from authentication if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authentication. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authentication.
LOCAL	Specifies the local user database.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authentication. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[-*port*] • **udp**/*port*[-*port*] • **icmp**/*type* • *protocol*[/*port*[-*port*]] Although you can configure the security appliance to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the security appliance allows other traffic requiring authentication. See "Usage Guidelines" for more information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To enable authentication for traffic that is specified by an access list, use the **aaa authentication match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authentication include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authentication match** command.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the security appliance to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the security appliance to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the security appliance allows other traffic requiring authentication.

The authentication ports that the security appliance supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the security appliance in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the security appliance username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the security appliance password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	4 tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the security appliance intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the security appliance intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the security appliance allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the security appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can authenticate with the security appliance directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the security appliance at the following URLs when you enable AAA for the interface:

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

Examples

The following example includes for authentication TCP traffic on the outside interface, with an inside IP address of 192.168.0.0 and a netmask of 255.255.0.0, with an outside IP address of all hosts, and using a server group named tacacs+. The second command line excludes Telnet traffic on the outside interface with an inside address of 192.168.38.0, with an outside IP address of all hosts:

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

The following examples demonstrate ways to use the *interface-name* parameter. The security appliance has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
hostname(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the inside network to the perimeter network:

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the inside network:

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the outside network to the perimeter network:

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

This example enables authentication for connections originated from the perimeter network to the outside network:

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

Related Commands

Command	Description
aaa authentication console	Enables authentication for management access.
aaa authentication match	Enables user authentication for through traffic.

aaa authentication secure-http-client	Provides a secure method for user authentication to the security appliance prior to allowing HTTP requests to traverse the security appliance.
aaa-server	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication listener

To enable HTTP(S) listening ports to authenticate network users, use the **aaa authentication listener** command in global configuration mode. When you enable a listening port, the security appliance serves an authentication page for direct connections and optionally for through traffic. To disable the listeners, use the **no** form of this command.

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

Syntax Description

http[s]	Specifies the protocol that you want to listen for, either HTTP or HTTPS. Enter this command separately for each protocol.
interface_name	Specifies the interface on which you enable listeners.
port *portnum*	Specifies the port number that the security appliance listens on for direct or redirected traffic; the defaults are 80 (HTTP) and 443 (HTTPS). You can use any port number and retain the same functionality, but be sure your direct authentication users know the port number; redirected traffic is sent to the correct port number automatically, but direct authenticators must specify the port number manually.
redirect	Redirects through traffic to an authentication web page served by the security appliance. Without this keyword, only traffic directed to the security appliance interface can access the authentication web pages.

Defaults

By default, no listener services are enabled, and HTTP connections use basic HTTP authentication. If you enable the listeners, the default ports are 80 (HTTP) and 443 (HTTPS).

If you are upgrading from 7.2(1), then the listeners are enabled on ports 1080 (HTTP) and 1443 (HTTPS). The **redirect** option is also enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

Without the **aaa authentication listener** command, when HTTP(S) users need to authenticate with the security appliance after you configure the **aaa authentication match** or **aaa authentication include** command, the security appliance uses basic HTTP authentication. For HTTPS, the security appliance generates a custom login screen.

If you configure the **aaa authentication listener** command with the **redirect** keyword, the security appliance redirects all HTTP(S) authentication requests to web pages served by the security appliance.

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

If you enter the **aaa authentication listener** command *without* the **redirect** option, then you only enable direct authentication with the security appliance, while letting through traffic use basic HTTP authentication. The **redirect** option enables both direct and through-traffic authentication. Direct authentication is useful when you want to authenticate traffic types that do not support authentication challenges; you can have each user authenticate directly with the security appliance before using any other services.

Note If you enable the **redirect** option, you cannot also configure static PAT for the same interface where you translate the interface IP address and the same port that is used for the listener; NAT succeds, but authentication fails. For example, the following configuration is unsupported:

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside redirect
```

The following configuration is supported; the listener uses port 1080 instead of the default 80:

```
hostname(config)# static (inside,outside) tcp interface www 192.168.0.50 www netmask
255.255.255.255
hostname(config)# aaa authentication listener http outside port 1080 redirect
```

Examples

The following example configures the security appliance to redirect HTTP and HTTPS connections to the default ports:

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

The following example allows authentication requests directly to the security appliance; through traffic uses basic HTTP authentication:

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

The following example configures the security appliance to redirect HTTP and HTTPS connections to non-default ports:

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

Related Commands

Command	Description
aaa authentication match	configures user authentication for through traffic.
aaa authentication secure-http-client	Enables SSL and secure username and password exchange between HTTP clients and the security appliance.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.
virtual http	Supports cascading HTTP authentications with basic HTTP authentication.

aaa authentication match

To enable authentication for connections through the security appliance, use the **aaa authentication match** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

Syntax Description

acl_name	Specifies an extended access list name.
interface_name	Specifies the interface name from which to authenticate users.
LOCAL	Specifies the local user database.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You cannot use the **aaa authentication match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the security appliance to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the security appliance to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the security appliance allows other traffic requiring authentication.

The authentication ports that the security appliance supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS (requires the **aaa authentication listener** command)

Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the security appliance in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the security appliance username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the security appliance password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> asa1@partreq
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	4 tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the security appliance intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the security appliance intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the security appliance allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the Security Appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can authenticate with the security appliance directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the security appliance at the following URLs when you enable AAA for the interface:

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

Examples

The following set of examples illustrates how to use the **aaa authentication match** command:

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)
```

```
hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

In this context, the following command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

is equivalent to this command:

```
hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

The **aaa** command statement list is order-dependent between **access-list** command statements. If you enter the following command:

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

before this command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

the security appliance tries to find a match in the **mylist access-list** command statement group before it tries to find a match in the **yourlist access-list** command statement group.

Related Commands

Command	Description
aaa authorization	Enables user authorization services.
access-list extended	Creates an access list.
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication secure-http-client

To enable SSL and secure username and password exchange between HTTP clients and the security appliance, use the **aaa authentication secure-http-client** command in global configuration mode. To disable this function, use the **no** form of this command. The **aaa authentication secure-http-client** command offers a secure method for user authentication to the security appliance prior to allowing user HTTP-based web requests to traverse the security appliance.

aaa authentication secure-http-client

no aaa authentication secure-http-client

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **aaa authentication secure-http-client command** secures HTTP client authentication (through SSL). This command is used for HTTP cut-through proxy authentication.

The **aaa authentication secure-http-client** command has the following limitations:

- At runtime, a maximum of 16 HTTPS authentication processes is allowed. If all 16 HTTPS authentication processes are running, the 17th, new HTTPS connection requiring authentication is not allowed.
- When **uauth timeout 0** is configured (the **uauth timeout** is set to 0), HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the **uauth timeout** to 1 second with the **timeout uauth 0:0:1** command. However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.

- Because HTTPS authentication occurs on the SSL port 443, users must not configure an **access-list** command statement to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port. In the following example, the first line configures static PAT for web traffic and the second line must be added to support the HTTPS authentication configuration:

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

Examples

The following example configures HTTP traffic to be securely authenticated:

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

where "..." represents your values for *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag*.

The following command configures HTTPS traffic to be securely authenticated:

```
hostname (config)# aaa authentication include https...
```

where "..." represents your values for *authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*.

Note The **aaa authentication secure-https-client** command is not needed for HTTPS traffic.

Related Commands

Command	Description
aaa authentication	Enables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command.
virtual telnet	Accesses the security appliance virtual server.

aaa authorization command

The **aaa authorization command** command specifies whether command execution at the CLI is subject to authorization. To enable command authorization, use the **aaa authorization command** command in global configuration mode. To disable command authorization, use the **no** form of this command.

aaa authorization command {LOCAL | *server_tag* [**LOCAL**]}

no aaa authorization command {**LOCAL |** *server_tag* [**LOCAL**]}

Syntax Description

LOCAL	Enables local command privilege levels set by the **privilege** command. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the security appliance places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user's privilege level and below. If you specify **LOCAL** after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
server_tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command.

Defaults

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Support added for fallback to LOCAL authorization when a TACACS+ server group is temporarily unavailable.
8.0(2)	Support for RADIUS and LDAP (mapped) users was added using the **LOCAL** keyword.

Usage Guidelines

By default when you log in, you can access user EXEC mode, which offers only minimal commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands. If you want to control the access to commands, the security appliance lets you configure command authorization, where you can determine which commands that are available to a user.

Supported Command Authorization Methods

You can use one of two command authorization methods:

- Local privilege levels—Configure the command privilege levels on the security appliance. When a local, RADIUS, or LDAP (if you map LDAP attributes to RADIUS attributes) user authenticates for CLI access, the security appliance places that user in the privilege level that is defined by the local database, RADIUS, or LDAP server. The user can access commands at the user's privilege level and below. Note that all users access user EXEC mode when they first log in (commands at level 0 or 1). The user needs to authenticate again with the **enable** command to access privileged EXEC mode (commands at level 2 or higher), or they can log in with the **login** command (local database only).

Note You can use local command authorization without any users in the local database and without CLI or enable authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the security appliance places you in level 15. You can then create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the security appliance places you in level *n*. These levels are not used unless you turn on local command authorization. (See the **enable** command for more information.)

- TACACS+ server privilege levels—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

  When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

  When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default "enable_15" username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

  This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.

  When configuring command authorization, consider the following:

  – An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.

– If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied use of commands that are also denied to administrators who are permitted use of the **changeto** command.

When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.

Note The system execution space does not support **aaa** commands; therefore, command authorization is not available in the system execution space.

Local Command Authorization Prerequisites

- Configure enable authentication for local, RADIUS, or LDAP authentication using the **aaa authentication enable console** command.

  Enable authentication is essential to maintain the username after the user accesses the **enable** command.

  Alternatively, you can use the **login** command (which is the same as the **enable** command with authentication), which requires no configuration. We do not recommend this option because it is not as secure as enable authentication.

  You can also use CLI authentication (**aaa authentication** {**ssh** | **telnet** | **serial**} **console**), but it is not required.

- For RADIUS and LDAP support, enter the **aaa authorization exec authentication-server** command. This command enables support of administrative user privilege levels from RADIUS. Without this command, the security appliance only supports privilege levels for local database users and defaults all other types of users to level 15.

  This command also enables management authorization for local, RADIUS, LDAP (mapped), and TACACS+ users.

- See the following prerequisites for each user type:
  - Local database users—Configure each user in the local database at a privilege level from 0 to 15 using the **username** command.
  - RADIUS users—Configure the user with Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15.
  - LDAP users—Configure the user with a privilege level between 0 and 15, and then map the LDAP attribute to Cisco VAS CVPN3000-Privilege-Level using the **ldap map-attributes** command.
- See the **privilege** command for information about setting command privilege levels.

TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the security appliance sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the security appliance.

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the security appliance. For example, in your TACACS+ server pool, include one server

connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels.

See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for information about configuring the TACACS+ server.

TACACS+ Command Authorization Prerequisites

- Configure CLI authentication using the **aaa authentication** {**ssh** | **telnet** | **serial**} **console** command.
- Configure **enable** authentication using the **aaa authentication enable console** command.

Examples

The following example shows how to enable command authorization using a TACACS+ server group named tplus1:

```
hostname(config)# aaa authorization command tplus1
```

The following example shows how to configure administrative authorization to support fallback to the local user database if all servers in the tplus1 server group are unavailable.

```
hostname(config)# aaa authorization command tplus1 LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables CLI, ASDM, and enable authentication.
aaa authorization exec authentication-server	Enables support of administrative user privilege levels from RADIUS.
aaa-server host	Configures host-related attributes.
aaa-server	Configures group-related server attributes.
enable	Enters privileged EXEC mode.
ldap map-attributes	Maps LDAP attributes to RADIUS attributes that the security appliance can use.
login	Enters privileged EXEC mode using the local database for authentication.
service-type	Limits local database user CLI, ASDM, and enable access.
show running-config aaa	Displays the AAA configuration.

aaa authorization exec authentication-server

To enable management authorization, and to enable support of administrative user privilege levels from RADIUS, use the **aaa authorization exec authentication-server** command in global configuration mode. User privilege levels are used for command authorization along with the locally-defined command levels. To disable management authorization and RADIUS user levels, use the **no** form of this command.

aaa authorization exec authentication-server

no aaa authorization exec authentication-server

Syntax Description

This command has no arguments or keywords.

Defaults

By default, this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If you configure **aaa authentication console** commands to authenticate users when they access the CLI, ASDM, or the **enable** command, then the **aaa authorization exec authentication-server** command can limit management access depending on the user configuration.

Note Serial access is not included in management authorization, so if you configure **aaa authentication serial console**, then any user who authenticates can access the console port.

To configure the user for management authorization, see the following requirements for each AAA server type or local user:

- RADIUS or LDAP (mapped) users—Use the IETF RADIUS numeric Service-Type attribute which maps to one of the following values. (To map LDAP attributes, see the **ldap attribute-map** command.)
  - Service-Type 6 (Administrative)—Allows full access to any services specified by the **aaa authentication console** commands.

  - Service-Type 7 (NAS prompt)—Allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh**} **console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure **enable** authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - Service-Type 5 (Outbound)—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed). Remote access (IPSec and SSL) users can still authenticate and terminate their remote access sessions.
- TACACS+ users—Authorization is requested with the "service=shell" and the server responds with PASS or FAIL.
  - PASS, privilege level 1—Allows full access to any services specified by the **aaa authentication console** commands.
  - PASS, privilege level 2 and higher—Allows access to the CLI when you configure the **aaa authentication** {**telnet | ssh**} **console** command, but denies ASDM configuration access if you configure the **aaa authentication http console** command. ASDM monitoring access is allowed. If you configure enable authentication with the **aaa authentication enable console** command, the user cannot access privileged EXEC mode using the **enable** command.
  - FAIL—Denies management access. The user cannot use any services specified by the **aaa authentication console** commands (excluding the **serial** keyword; serial access is allowed).
- Local users—Set the **service-type** command. By default, the **service-type** is **admin**, which allows full access to any services specified by the **aaa authentication console** commands.

The **aaa authorization exec authentication-server** command also enables support of administrative user privilege levels from RADIUS. When you enter the **aaa authorization command LOCAL** command, local users, RADIUS users, and LDAP (mapped) users use the locally-defined privilege levels set by the **privilege** command. See the following prerequisites for each user type:

- RADIUS users—Configure the user with Cisco VSA CVPN3000-Privilege-Level with a value between 0 and 15.
- LDAP users—Configure the user with a privilege level between 0 and 15, and then map the LDAP attribute to Cisco VAS CVPN3000-Privilege-Level according to the **ldap attribute-map** command.

Examples

The following example shows use of the **aaa authentication console** command for a Telnet connection to a RADIUS server with the server tag "radius":

```
hostname(config)# aaa authentication telnet console radius
```

The following example identifies the server group "AuthIn" for enable authentication.

```
hostname(config)# aaa authentication enable console AuthIn
```

The following example shows use of the **aaa authentication console** command with fallback to the LOCAL user database if all the servers in the group "svrgrp1" fail:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication console	Enables console authentication.
ldap attribute-map	Maps LDAP attributes.
service-type	Limits a local user CLI access.
show running-config aaa	Display the AAA configuration.

aaa authorization include, exclude

To enable authorization for connections through the security appliance, use the **aaa authorization include** command in global configuration mode. To exclude addresses from authorization, use the **aaa authorization exclude** command. To disable authorization, use the **no** form of this command.

aaa authorization {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from authorization if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authorization. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authorization.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authorization. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ssh** • **telnet** • **tcp**/*port*[-*port*] • **udp**/*port*[-*port*] • **icmp**/*type* • *protocol*[/*port*[-*port*]] **Note** Specifying a port range might produce unexpected results at the authorization server. The security appliance sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Defaults

An IP address of **0** means "all hosts." Setting the local IP address to **0** lets the authorization server decide which hosts are authorized.

Fallback to the local database for authorization is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The **exclude** parameter now allows the user to specify a port to exclude to a specific host or hosts.

Usage Guidelines

To enable authorization for traffic that is specified by an access list, use the **aaa authorization match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authorization include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authorization match** command.

You can configure the security appliance to perform network access authorization with TACACS+. Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the security appliance. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the security appliance checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the security appliance sends the username to the TACACS+ server. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile. The security appliance enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

For each IP address, one **aaa authorization include** command is permitted.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

Note Specifying a port range might produce unexpected results at the authorization server. The security appliance sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the TACACS+ protocol:

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication ssh console tplus1
```

In this example, the first command statement creates a server group named tplus1 and specifies the TACACS+ protocol for use with this group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next three command statements specify that any users starting connections through the outside interface to any foreign host will be authenticated using the tplus1 server group, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that SSH access to the security appliance console requires authentication from the tplus1 server group.

The following example enables authorization for DNS lookups from the outside interface:

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

This means that users cannot ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization only for ICMP echoes (pings) that arrive at the inside interface from an inside host:

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

Related Commands

Command	Description
aaa authorization command	Specifies whether command execution is subject to authorization, or configure administrative authorization to support fallback to the local user database if all servers in the specified server group are disabled.
aaa authorization match	Enables or disables the LOCAL or TACACS+ user authorization services for a specific access-list command name.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authorization match

To enable authorization for connections through the security appliance, use the **aaa authorization match** command in global configuration mode. To disable authorization, use the **no** form of this command.

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies an extended access list name. See the **access-list extended** command. The **permit** ACEs mark matching traffic for authorization, while **deny** entries exclude matching traffic from authorization.
interface_name	Specifies the interface name from which users require authentication.
server_tag	Specifies the AAA server group tag as defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You cannot use the **aaa authorization match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You can configure the security appliance to perform network access authorization with TACACS+. RADIUS authorization with the **aaa authorization match** command only supports authorization of VPN management connections to the FWSM.

Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the security appliance. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the security appliance checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the security appliance sends the username to the TACACS+ server. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile. The security appliance enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

```
Unable to connect to remote host: Connection timed out
```

Note Specifying a port range might produce unexpected results at the authorization server. The security appliance sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the tplus1 server group with the **aaa** commands:

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization match myacl inside tplus1
```

In this example, the first command statement defines the tplus1 server group as a TACACS+ group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next two command statements specify that any connections traversing the inside interface to any foreign host are authenticated using the tplus1 server group, and that all these connections are logged in the accounting database. The last command statement specifies that any connections that match the ACEs in myacl are authorized by the AAA servers in the tplus1 server group.

Related Commands

Command	Description
aaa authorization	Enable or disable user authorization.
clear configure aaa	Reset all aaa configuration parameters to the default values.
clear uauth	Delete AAA authorization and authentication caches for one user or all users, which forces users to reauthenticate the next time that they create a connection.
show running-config aaa	Display the AAA configuration.
show uauth	Display the username provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is only authenticated or has cached services.

aaa local authentication attempts max-fail

To limit the number of consecutive failed local login attempts that the security appliance allows any given user account (with the exception of users with a privilege level of 15; this feature does not affect level 15 users), use the **aaa local authentication attempts max-fail** command in global configuration mode. This command only affects authentication with the local user database. To disable this feature and allow an unlimited number of consecutive failed local login attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number*

Syntax Description

number	The maximum number of times a user can enter a wrong password before being locked out. This number can be in the range 1-16.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you omit this command, there is no limit on the number of times a user can enter an incorrect password.

After a user makes the configured number of attempts with the wrong password, the user is locked out and cannot log in successfully until the administrator unlocks the username. Locking or unlocking a username results in a system log message.

Users with a privilege level of 15 are not affected by this command; they cannot be locked out.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the security appliance reboots.

Examples

The following example shows use of the **aaa local authentication attempts max-limits** command to set the maximum number of failed attempts allowed to 2:

```
hostname(config)# aaa local authentication attempts max-limits 2
hostname(config)#
```

Related Commands

Command	Description
clear aaa local user lockout	Clears the lockout status of the specified users and set their failed-attempts counter to 0.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user's locked-out status.
show aaa local user	Shows the list of usernames that are currently locked.

aaa mac-exempt

To specify the use of a predefined list of MAC addresses to exempt from authentication and authorization, use the **aaa mac-exempt** command in global configuration mode. You can only add one **aaa mac-exempt** command. To disable the use of a list of MAC addresses, use the **no** form of this command.

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

Syntax Description

id	Specifies a MAC list number configured with the **mac-list** command.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Configure the MAC list number using the **mac-list** command before using the **aaa mac-exempt** command. Permit entries in the MAC list exempt the MAC addresses from authentication and authorization, while deny entries require authentication and authorization for the MAC address, if enabled. Because you can only add one instance of the **aaa mac-exempt** command, be sure that your MAC list includes all the MAC addresses you want to exempt.

Examples

The following example bypasses authentication for a single MAC address:

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2:

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.
mac-list	Specifies a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization.

aaa proxy-limit

To manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user, use the **aaa proxy-limit** command in global configuration mode. To disable proxies, use the **disable** parameter. To return to the default proxy-limit value (16), use the **no** form of this command.

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

Syntax Description

disable	No proxies allowed.
proxy_limit	Specify the number of concurrent proxy connections allowed per user, from 1 to 128.

Defaults

The default proxy-limit value is 16.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

Examples

The following example shows how to set the maximum number of outstanding authentication requests allowed per user:

```
hostname(config)# aaa proxy-limit 6
```

Related Commands

Command	Description
aaa authentication	Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication
aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa-server

To create a AAA server group and configure AAA server parameters that are group-specific and common to all group hosts, use the **aaa-server** command in global configuration mode. To remove the designated group, use the **no** form of this command.

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

Syntax Description

server-tag	Specifies the server group name, which is matched by the name specified by the **aaa-server host** commands. Other AAA commands make reference to the AAA server group name.
protocol *server-protocol*	Specifies the AAA protocol that the servers in the group support: • **http-form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	The http-form protocol was added.

Usage Guidelines

You control AAA server configuration by defining a AAA server group protocol with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command.

You can have up to 15 server groups in single mode or 4 server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

Examples

The following example shows the use of the **aaa-server** command to modify details of a TACACS+ server group configuration:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
```

Related Commands

Command	Description
accounting-mode	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
reactivation-mode	Specifes the method by which failed servers are reactivated.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

aaa-server active, fail

To reactivate a AAA server that is marked failed, use the **aaa-server active** command in privileged EXEC mode. To fail an active server, use the **aaa-server fail** command in privileged EXEC mode.

aaa-server *server_tag* [**active | fail**] **host** {*server_ip* | *name*}

Syntax Description

active	Sets the server to an active state.
fail	Sets the server to a failed state.
host	Specifies the host IP address name or IP address.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server_ip	Specifies the IP address of the AAA server.
server_tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Without this command, servers in a group that failed remain in a failed state until all servers in the group fail, after which all are reactivated.

Examples

The following example shows the state for server 192.168.125.60, and manually reactivates it:

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: FAILED. Server disabled at 11:10:08 UTC  Fri Aug 22
...
hostname# aaa-server active host 192.168.125.60
```

```
hostname# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE (admin initiated). Last Transaction at 11:40:09 UTC  Fri Aug 22
...
```

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

aaa-server host

To configure a AAA server as part of a AAA server group and to configure AAA server parameters that are host-specific, use the **aaa-server host** command in global configuration mode. When you use the **aaa-server host** command, you enter the aaa-server host configuration mode, from which you can specify and manage host-specific AAA server connection data. To remove a host configuration, use the **no** form of this command.

aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

Syntax Description

(*interface-name***)**	(Optional) Specifies the network interface where the authentication server resides. The parentheses are required in this parameter. If you do not specify an interface, the default is **inside**, if available.
key	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters entered past 127 are ignored. The key is used between the security appliance and the server for encrypting data between them. the key must be the same on both the security appliance and server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in host mode.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server-ip	Specifies the IP address of the AAA server.
server-tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server** command.
timeout *seconds*	(Optional) The timeout interval for the request. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server. You can modify the timeout interval using the **timeout** command in host mode.

Defaults

The default timeout value is 10 seconds.

The default interface is inside.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	Support for DNS names was added.

Usage Guidelines

You control AAA server configuration by defining a AAA server group with the **aaa-server** command, and then you add servers to the group using the **aaa-server host** command.

You can have up to 15 server groups in single mode or 4 server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

After you enter the **aaa-server host** command, you can configure host-specific parameters.

Examples

The following example configures a Kerberos AAA server group named “watchdogs”, adds a AAA server to the group, and defines the Kerberos realm for the server.

Note Kerberos realm names use numbers and upper-case letters only. Although the security appliance accepts lower-case letters for a realm name, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

The following example configures an SDI AAA server group named “svrgrp1”, and then adds a AAA server to the group, sets the timeout interval to 6 seconds, sets the retry interval to 7 seconds, and configures the SDI version to version 5.

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

Related Commands

Command	Description
aaa-server	Creates and modifies AAA server groups.
clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

absolute

To define an absolute time when a time range is in effect, use the **absolute** command in time-range configuration mode. To disable, use the **no** form of this command.

absolute [**end** *time date*] [**start** *time date*]

no absolute

Syntax Description

date	Specifies the date in the format day month year; for example, 1 January 2006. The valid range of years is 1993 through 2035.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

Defaults

If no start time and date are specified, the permit or deny statement is in effect immediately and always on. Similarly, the maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

Examples

The following example activates an ACL at 8:00 a.m. on 1 January 2006:

```
hostname(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

Related Commands

Command	Description
access-list extended	Configures a policy for permitting or denying IP traffic through the security appliance.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the security appliance based on time.

accept-subordinates

To configure the security appliance to accept subordinate CA certificates if delivered during phase one IKE exchange when not previously installed on the device, use the **accept-subordinates** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

accept-subordinates

no accept-subordinates

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is on (subordinate certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

During phase 1 processing, an IKE peer might pass both a subordinate certificate and an identity certificate. The subordinate certificate might not be installed on the security appliance. This command lets an administrator support subordinate CA certificates that are not configured as trustpoints on the device without requiring that all subordinate CA certificates of all established trustpoints be acceptable; in other words, this command lets the device authenticate a certificate chain without installing the entire chain locally.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and allows the security appliance to accept subordinate certificates for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

access-group

To bind an access list to an interface, use the **access-group** command in global configuration mode. To unbind an access list from the interface, use the **no** form of this command.

access-group *access-list* {**in | out**} **interface** *interface_name* [**per-user-override** | **control-plane**]

no access-group *access-list* {**in | out**} **interface** *interface_name*

Syntax Description

access-list	Access list *id.*
control-plane	(Optional) Specifies if the rule is for to-the-box traffic.
in	Filters the inbound packets at the specified interface.
interface *interface-name*	Name of the network interface.
out	Filters the outbound packets at the specified interface.
per-user-override	(Optional) Allows downloadable user access lists to override the access list applied to the interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **access-group** command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the security appliance continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the security appliance discards the packet and generates the following syslog message.

```
%hostname-4-106019: IP packet from source_addr to destination_addr, protocol
protocol received from interface interface_name deny by access-group id
```

The *per-user-override* option allows downloaded access lists to override the access list applied to the interface. If the *per-user-override* optional argument is not present, the security appliance preserves the existing filtering behavior. When *per-user-override* is present, the security appliance allows the **permit**

or **deny** status from the per-user access-list (if one is downloaded) associated to a user to override the permit or deny status from the **access-group** command associated access list. Additionally, the following rules are observed:

- At the time a packet arrives, if there is no per-user access list associated with the packet, the interface access list will be applied.
- The per-user access list is governed by the timeout value specified by the **uauth** option of the **timeout** command but it can be overridden by the AAA per-user session timeout value.
- Existing access list log behavior will be the same. For example, if user traffic is denied because of a per-user access list, syslog message 109025 will be logged. If user traffic is permitted, no syslog message is generated. The log option in the per-user access-list will have no effect.

Always use the **access-list** command with the **access-group** command.

The **access-group** command binds an access list to an interface. The **in** keyword applies the access list to the traffic on the specified interface. The **out** keyword applies the access list to the outbound traffic.

Note If all of the functional entries (the permit and deny statements) are removed from an access list that is referenced by one or more **access-group** commands, the **access-group** commands are automatically removed from the configuration. The **access-group** command cannot reference empty access lists or access lists that contain only a remark.

The **no access-group** command unbinds the access list from the interface *interface_name*.

The **show running config access-group** command displays the current access list bound to the interfaces.

The **clear configure access-group** command removes all the access lists from the interfaces.

Note Access control rules for to-the-box management traffic (defined by such commands as **http**, **ssh**, or **telnet**) have higher precedence than an access list applied with the **control-plane** option. Therefore, such permitted management traffic will be allowed to come in even if explicitly denied by the to-the-box access list.

Examples

The following example shows how to use the **access-group** command:

```
hostname(config)# static (inside,outside) 209.165.201.3 10.1.1.3
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

The **static** command provides a global address of 209.165.201.3 for the web server at 10.1.1.3. The **access-list** command lets any host access the global address using port 80. The **access-group** command specifies that the **access-list** command applies to traffic entering the outside interface.

Related Commands

Command	Description
access-list extended	Creates an access list, or uses a downloadable access list.
clear configure access-group	Removes access groups from all the interfaces.
show running-config access-group	Displays the context group members.

access-list alert-interval

To specify the time interval between deny flow maximum messages, use the **access-list alert-interval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list alert-interval *secs*

no access-list alert-interval

Syntax Description

secs	Time interval between deny flow maximum message generation; valid values are from 1 to 3600 seconds. The default value is 300 seconds.

Defaults

The default is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **access-list alert-interval** command sets the time interval for generating the system log message 106001. The system log message 106001 alerts you that the adaptive security appliance has reached a deny flow maximum. When the deny flow maximum is reached, another system log message 106001 is generated if at least *secs* seconds have passed since the last 106001 message was generated.

See the **access-list deny-flow-max** command for information about the deny flow maximum message generation.

Examples

The following example shows how to specify the time interval between deny flow maximum messages:

```
hostname(config)# access-list alert-interval 30
```

Related Commands

Command	Description
access-list deny-flow-max	Specifies the maximum number of concurrent deny flows that can be created.
access-list extended	Adds an access list to the configuration and is used to configure policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.

access-list deny-flow-max

To specify the maximum number of concurrent deny flows that can be created, use the **access-list deny-flow-max** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list deny-flow-max

no access-list deny-flow-max

Syntax Description

This command has no arguments or keywords.

Defaults

The default is 4096 concurrent deny flows.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

System log message 106101 is generated when the adaptive security appliance has reached the maximum number, *n*, of ACL deny flows.

Examples

The following example shows how to specify the maximum number of concurrent deny flows that can be created:

```
hostname(config)# access-list deny-flow-max 256
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and is used to configure policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.

Command	Description
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list ethertype

To configure an access list that controls traffic based on its EtherType, use the **access-list ethertype** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

Syntax Description

any	Specifies access to anyone.
bpdu	Specifies access to bridge protocol data units. By default, BPDUs are denied.
deny	Denies access if the conditions are matched.
hex_number	Indicates a 16-bit hexadecimal number greater than or equal to 0x600, by which an EtherType can be identified.
id	Lists the name or number of an access list.
ipx	Specifies access to IPX.
mpls-multicast	Specifies access to MPLS multicast.
mpls-unicast	Specifies access to MPLS unicast.
permit	Permits access if the conditions are matched.

Defaults

The defaults are as follows:

- The adaptive security appliance denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates system log message 106023 for denied packets—deny packets must be present to log denied packets.

When the **log** optional keyword is specified, the default severity level for system log message 106100 is 6 (informational).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The adaptive security appliance can control any EtherType identified by a 16-bit hexadecimal number. EtherType ACLs support Ethernet V2 frames. The 802.3-formatted frames are not handled by the ACL, because they use a length field instead of a type field. Bridge protocol data units, which are handled by the ACL, are the only exception; they are SNAP-encapsulated, and the adaptive security appliance is designed to specifically handle BPDUs.

Because EtherTypes are connectionless, you need to apply the ACL to both interfaces if you want traffic to pass in both directions.

If you allow MPLS, ensure that LDP and TDP TCP connections are established through the adaptive security appliance by configuring both MPLS routers connected to the adaptive security appliance to use the IP address on the adaptive security appliance interface as the router-ID for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

You can apply only one ACL of each type (extended and EtherType) to each direction of an interface. You can also apply the same ACLs on multiple interfaces.

Note If an EtherType access list is configured with the **deny all** command, all Ethernet frames are discarded. Only physical protocol traffic, such as auto-negotiation, is still allowed.

Examples

The following example shows how to add an EtherType access list:

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

Related Commands

Command	Description
access-group	Binds the access list to an interface.
clear access-group	Clears access list counters.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list extended

To add an Access Control Entry, use the **access-list extended** command in global configuration mode. An access list is made up of one or more ACEs with the same access list ID. Access lists are used to control network access or to specify traffic for many features to act upon. To remove an ACE, use the **no** form of this command. To remove the entire access list, use the **clear configure access-list** command.

access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**}
{*protocol* | **object-group** *protocol_obj_grp_id*}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

no access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**} {**tcp** | **udp**}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port*] | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

Syntax Description

default	(Optional) Sets logging to the default method, which is to generate system log message 106023 for each denied packet.
deny	Denies a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword prevents the packet from passing through the adaptive security appliance. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword exempts the traffic from inspection. Some features do not allow deny ACEs to be used, such as NAT. See the command documentation for each feature that uses an access list for more information.
dest_ip	Specifies the IP address of the network or host to which the packet is being sent. Enter the **host** keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the **any** keyword instead of the address and mask to specify any address.
disable	(Optional) Disables logging for this ACE.
extended	(Optional) Adds an ACE.
icmp_type	(Optional) If the protocol is ICMP, specifies the ICMP type.
id	Specifies the access list ID, as a string or integer up to 241 characters in length. The ID is case-sensitive. **Tip** Use all capital letters to see the access list ID better in your configuration.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.

interface *ifc_name*	Specifies the interface address as the source or destination address. **Note** You must specify the interface keyword instead of specifying the actual IP address in the access list when the traffic destination is a device interface.
interval *secs*	(Optional) Specifies the log interval at which to generate system log message 106100. Valid values are from 1 to 600 seconds. The default is 300.
level	(Optional) Sets the system log message 106100 severity level from 0 to 7. The default level is 6 (informational).
line *line-num*	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.
log	(Optional) Sets logging options when a **ACE** matches a packet for network access (an access list applied with the **access-group** command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, then the default system log message 106023 is generated.
mask	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The adaptve security appliance uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
object-group *icmp_type_obj_grp_id*	(Optional) If the protocol is ICMP, specifies the identifier of an ICMP-type object group. See the **object-group icmp-type** command to add an object group.
object-group *network_obj_grp_id*	Specifies the identifier of an network object group. See the **object-group network** command to add an object group.
object-group *protocol_obj_grp_id*	Specifies the identifier of a protocol object group. See the **object-group protocol** command to add an object group.
object-group *service_obj_grp_id*	(Optional) If you set the protocol to TCP or UDP, specifies the identifier of a service object group. See the **object-group service** command to add an object group.
operator	(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows: • **lt**—less than • **gt**—greater than • **eq**—equal to • **neq**—not equal to • **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200`

permit	Permits a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword lets the packet pass through the adaptive security appliance. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword applies inspection to the packet.
port	(Optional) If you set the protocol to TCP or UDP, specifies the integer or name of a TCP or UDP port. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
protocol	Specifies the IP protocol name or number. For example, UDP is 17, TCP is 6, and EGP is 47.
src_ip	Specifies the IP address of the network or host from which the packet is being sent. Enter the **host** keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the **any** keyword instead of the address and mask to specify any address.
time-range *time_range_name*	(Optional) Schedules each ACE to be activated at specific times of the day and week by applying a time range to the ACE. See the **time-range** command for information about defining a time range.

Defaults

The defaults are as follows:

- ACE logging generates system log message 106023 for denied packets. A **deny ACE** must be present to log denied packets.
- When the **log** keyword is specified, the default level for system log message 106100 is 6 (informational), and the default interval is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Each ACE that you enter for a given access list name is appended to the end of the access list, unless you specify the line number in the ACE.

The order of ACEs is important. When the adaptive security appliance decides whether to forward or drop a packet, the adaptive security appliance tests the packet with each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are ever checked.

Access lists have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the adaptive security appliance except for particular addresses, then you need to deny the particular addresses and permit all others.

When you use NAT, the IP addresses you specify for an access list depend on the interface to which the access list is attached; you need to use addresses that are valid on the network connected to the interface. This guideline applies for both inbound and outbound access groups—the direction does not determine the address used, only the interface does.

For TCP and UDP connections, you do not need an access list to allow returning traffic, because the FWSM allows all returning traffic for established, bidirectional connections. For connectionless protocols such as ICMP, however, the adaptive security appliance establishes unidirectional sessions, so you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections.

Because ICMP is a connectionless protocol, you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as stateful connections. To control pinging, specify **echo-reply** (**0**) (adaptive security appliance to host) or **echo** (**8**) (host to adaptiv security appliance). See Table 1 for a list of ICMP types.

You can apply only one access list of each type (extended and EtherType) to each direction of an interface. You can apply the same access lists on multiple interfaces. See the **access-group** command for more information about applying an access list to an interface.

Note If you change the access list configuration, and you do not want to wait for existing connections to time out before the new access list information is used, you can clear the connections using the **clear local-host** command.

Table 1 lists the possible ICMP types values.

Table 2-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request

Table 2-1 ICMP Type Literals (continued)

ICMP Type	Literal
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

Examples

The following access list allows all hosts (on the interface to which you apply the access list) to go through the adaptive security appliance:

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following sample access list prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network. All other addresses are permitted.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to only some hosts, then enter a limited **permit ACE**. By default, all other traffic is denied unless explicitly permitted.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

The following access list restricts all hosts (on the interface to which you apply the access list) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following access list that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

To temporarily disable an access list that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based access list, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended** command to bind the time range to an access list. The following example binds an access list named “Sales” to a time range named “New_York_Minute”:

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

See the **time-range** command for more information about how to define a time range.

Related Commands

Command	Description
access-group	Binds the access list to an interface.
clear access-group	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays ACEs by number.
show running-config access-list	Displays the current running access-list configuration.

access-list remark

To specify the text of a remark to add before or after an **access-list extended** command, use the **access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** [*text*]

Syntax Description

id	Name of an access list.
line *line-num*	(Optional) The line number at which to insert a remark or an access control element (ACE).
remark text	Text of the remark to add before or after an **access-list extended** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The remark text must contain at least one non-space character; an empty remark is not allowed. The remark text can be up to 100 characters long, including spaces and punctuation.

You cannot use the **access-group** command on an ACL that includes a remark only.

Examples

The following example shows how to specify the text of a remark to add before or after an **access-list** command:

```
hostname(config)# access-list 77 remark checklist
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and is used to configure policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list rename

To rename an access list, use the **access-list rename** command in global configuration mode.

access-list *id* **rename** *new_acl_id*

Syntax Description

id	Name of an existing access list.
rename *new_acl_id*	Specifies the new access list ID, as a string or integer up to 241 characters long. The ID is case-sensitive.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If the access list is renamed to the same name, the adaptive security appliance will silently ignore the command.

Examples

The following example shows how to rename an access list from TEST to OUTSIDE:

```
hostname(config)# access-list TEST rename OUTSIDE
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and is used to configure policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list standard

To add an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution, use the **access-list standard** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

Syntax Description

any	Specifies access to anyone.
deny	Denies access if the conditions are matched.
host *ip_address*	Specifies access to a host IP address (optional).
id	Name or number of an access list.
ip_address ip_mask	Specifies access to a specific IP address (optional) and subnet mask.
line *line-num*	(Optional) The line number at which to insert an ACE.
permit	Permits access if the conditions are matched.

Defaults

The defaults are as follows:

- The adaptive security appliance denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates system log message 106023 for denied packets—deny packets must be present to log denied packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When used with the **access-group** command, the **deny** keyword does not allow a packet to traverse the adaptive security appliance. By default, the adaptive security appliance denies all packets on the originating interface unless you specifically permit access.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0.
- Use the **host** *ip_address* option as an abbreviation for a mask of 255.255.255.255.

Examples

The following example shows how to deny IP traffic through the adaptive security appliance:

```
hostname(config)# access-list 77 standard deny
```

The following example shows how to permit IP traffic through the adaptive security appliance if conditions are matched:

```
hostname(config)# access-list 77 standard permit
```

The following example shows how to specify a destination address:

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list webtype

To add an access list to the configuration that supports filtering for clientless SSL VPN, use the **access-list webtype** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

Syntax Description

any	Specifies all IP addresses.
any	(Optional) Specifies all URLs.
deny	Denies access if the conditions are matched.
host *ip_address*	Specifies a host IP address.
id	Name or number of an access list.
interval *secs*	(Optional) Specifies the time interval at which to generate system log message 106100; valid values are from 1 to 600 seconds.
ip_address ip_mask	Specifies a specific IP address and subnet mask.
log [[**disable** | **default**] | *level*]	(Optional) Specifies that system log message 106100 is generated for the ACE. See the **log** command for information.
oper	Compares *ip_address* ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
permit	Permits access if the conditions are matched.
port	Specifies the decimal number or name of a TCP or UDP port.
time_range *name*	(Optional) Specifies a keyword for attaching the time-range option to this access list element.
url	Specifies that a URL be used for filtering.
url_string	(Optional) Specifies the URL to be filtered.

Defaults

The defaults are as follows:

- The adaptive security appliance denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates system log message 106023 for denied packets—deny packets must be present to log denied packets.
- When the **log** optional keyword is specified, the default level for system log message 106100 is 6 (informational).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global Configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **access-list webtype** command is used to configure clientless SSL VPN filtering. The URL specified may be full or partial (no file specified), may include wildcards for the server, or may specify a port.

Valid protocol identifiers are: http, https, cifs, imap4, pop3, and smtp. The URL may also contain the keyword **any** to refer to any URL. An asterisk may be used to refer to a subcomponent of a DNS name.

Examples

The following example shows how to deny access to a specific company URL:

```
hostname(config)# access-list acl_company webtype deny url http://*.company.com
```

The following example shows how to deny access to a specific file:

```
hostname(config)# access-list acl_file webtype deny url
https://www.company.com/dir/file.html
```

The following example shows how to deny HTTP access to any URL through port 8080:

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
show running-config access-list	Displays the access-list configuration running on the adaptive security appliance.

accounting-mode

To indicate whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode), use the **accounting-mode** command in aaa-server configuration mode. To remove the accounting mode specification, use the **no** form of this command.

accounting-mode {**simultaneous** | **single**}

Syntax Description

simultaneous	Sends accounting messages to all servers in the group.
single	Sends accounting messages to a single server.

Defaults

The default value is single mode.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the keyword **single** to send accounting messages to a single server. Use the keyword **simultaneous** to send accounting messages to all servers in the server group.

This command is meaningful only when the server group is used for accounting (RADIUS or TACACS+).

Examples

The following example shows the use of the **accounting-mode** command to send accounting messages to all servers in the group:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.

aaa-server protocol	Enters AAA server group configuration mode, so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-port

To specify the port number used for RADIUS accounting for this host, use the **accounting-port** command in aaa-server host configuration mode. To remove the authentication port specification, use the **no** form of this command. This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to send accounting records.

accounting-port *port*

no accounting-port

Syntax Description

port	A port number for RADIUS accounting; the range of values is 1- 65535.

Defaults

By default, the device listens for RADIUS on port 1646 for accounting (in compliance with RFC 2058). If the port is not specified, the RADIUS accounting default port number (1646) is used.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If your RADIUS accounting server uses a port other than 1646, you must configure the security appliance for the appropriate port prior to starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures accounting port 2222.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Keeps a record of which network services a user has accessed.
aaa-server host	Enters AAA server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

accounting-server-group

To specify the AAA server group for sending accounting records use the **accounting-server-group** command in various modes. To remove accounting servers from the configuration, use the **no** form of this command. The security appliance uses accounting to keep track of the network resources that users access.

accounting-server-group *group_tag*

no accounting-server-group [*group_tag***]**

Syntax Description

group_tag	Identifies the previously configured accounting server or group of servers. Use the **aaa-server** command to configure accounting servers.

Defaults

No accounting servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command is now available in tunnel-group general-attributes configuration mode, instead of webvpn configuration mode.

Usage Guidelines

If you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes configuration mode.

Examples

The following example entered in tunnel-group-general attributes configuration mode, configures an accounting server group named “aaa-server123” for an IPSec LAN-to-LAN tunnel group “xyz”:

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general-attributes
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)#
```

The following example shows how to configure POP3S e-mail proxy to use the set of accounting servers named POP3SSVRS:

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

Related Commands

Command	Description
aaa-server	Configures authentication, authorization, and accounting servers.

CHAPTER 3

acl-netmask-convert through auto-update timeout Commands

acl-netmask-convert

Use the **acl-netmask-convert** command in aaa-server host configuration mode to specify how the security appliance treats netmasks received in a downloadable ACL from a RADIUS server which is accessed by using the **aaa-server host** command. Use the **no** form of this command to remove the speciied behavior for the security appliance.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

Syntax Description

auto-detect	Specifies that the security appliance should attempt to determine the type of netmask expression used. If it detects a wildcard netmask expression, it converts it to a standard netmask expression. See "Usage Guidelines" for more information about this keyword.
standard	Specifies that the security appliance assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.
wildcard	Specifies that the security appliance assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and it converts them all to standard netmask expressions when the ACLs are downloaded.

Defaults

By default, no conversion from wildcard netmask expressions is performed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server configuration host	•	•	•	•	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

Use the **acl-netmask-convert** command with the wildcard or auto-detect keywords when a RADIUS server provides downloadable ACLs that contain netmasks in wildcard format. The security appliance expects downloadable ACLs to contain standard netmask expressions whereas Cisco VPN 3000 series concentrators expect downloadable ACLs to contain wildcard netmask expressions, which are the reverse of a standard netmas expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match.The **acl-netmask-convert** command helps minimize the effects of these differences upon how you configure downloadable ACLs on your RADIUS servers.

The **auto-detect** keyword is helpful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with "holes" in them cannot be unambiguously detected and converted. For example, the wildcard netmask 0.0.255.0 permits anything in the third octet and can be used validly on Cisco VPN 3000 series concentrators, but the security appliance may not detect this expression as a wildcard netmask.

Examples

The following example configures a RADIUS AAA server named "srvgrp1" on host "192.168.3.4", enables conversion of downloadable ACL netmasks, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650:

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication.
aaa-server host	Enters aaa-server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

action

To either apply access policies to a session or teminate the session, use the **action** command in dynamic-access-policy-record configuration mode.

To reset the session to apply an access policy to a session, use the **no** form of the command.

action {continue | terminate}

no action {continue | terminate}

Syntax Description

continue	Applies the access policies to the session.
terminate	Terminates the connection.

Defaults

The default value is continue.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dynamic-access-policy- record configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **continue** keyword to apply the access policies to the session in all of the selected DAP records. Use the **terminate** keyword to terminate the connection in any of the selected DAP records.

Examples

The following example shows how to terminate a session for the DAP policy Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# action terminate
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

action-uri

To specify a web server URI to receive a username and password for single sign-on authentication, use the **action-uri** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command. Use the **no** form of the command to reset the URI parameter value, .

action-uri *string*

no action-uri

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The URI for an authentication program. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for the complete URI is 2048 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

A URI or Uniform Resource Identifier is a compact string of characters that identifies a point of content on the Internet, whether it be a page of text, a video or sound clip, a still or animated image, or a program. The most common form of URI is the web page address, which is a particular form or subset of URI called a URL.

The WebVPN server of the security appliance can use a POST request to submit a single sign-on authentication request to an authenticating web server. To accomplish this, configure the security appliance to pass a username and a password to an action URI on an authenticating web server using an HTTP POST request. The **action-uri** command specifies the location and name of the authentication program on the web server to which the security appliance sends the POST request.

You can discover the action URI on the authenticating web server by connecting to the web server login page directly with a browser. The URL of the login web page displayed in your browser is the action URI for the authenticating web server.

For ease of entry, you can enter URIs on multiple, sequential lines. The security appliance then concatenates the lines into the URI as you enter them. While the maximum characters per action-uri line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a CTRL-v escape sequence.

Examples

The following example specifies the URI on www.example.com:

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

```
hostname(config)# aaa-server testgrp1 host www.example.com
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

Note You must include the hostname and protocol in the action URI. In the preceding example, these are included in http://www.example.com at the start of the URI.

Related Commands

Command	Description
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the SSO server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

activation-key

To change the activation key on the security appliance and check the activation key running on the security appliance against the activation key that is stored as a hidden file in the Flash partition of the security appliance, use the **activation-key** command in global configuration mode. Use the **no** form of this command to deactivate the specified activation key running on the security appliance.

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

no activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

Syntax Description

activation-key-four-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.
activation-key-five-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration mode	•	•	•		•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexidecimal string withe one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

The key is not stored in the configuration file. The key is tied to the serial number.

Examples

The following example shows how to change the activation key on the security appliance:

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

Related Commands

Command	Description
show activation-key	Displays the activation key.

activex-relay

To enable or disable ActiveX controls on WebVPN sessions, use the **activex-relay** command in group-policy webvpn configuration mode or username webvpn configuration mode. Use the **no** form of this command to inherit the **activex-relay** command from the default group policy.

activex-relay {**enable** | **disable**}

no activex-relay

Syntax Description

enable	Enables ActiveX on WebVPN sessions.
disable	Disables ActiveX on WebVPN sessions.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration	•	—	•	—	—
Username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **activex-relay enable** command to let users launch Microsoft Office applications from the WebVPN browser. These applications use the WebVPN session to download and upload Microsoft Office documents. The ActiveX relay remains in force until the WebVPN session closes.

Examples

The following commands enable ActiveX controls on WebVPN sessions associated with a given group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# activex-relay enable
hostname(config-group-webvpn)
```

The following commands disable ActiveX controls on WebVPN sessions associated with a given username:

```
hostname(config-username-policy)# webvpn
hostname(config-username-webvpn)# activex-relay disable
```

```
hostname(config-username-webvpn)
```

address-pool (tunnel-group general attributes mode)

To specify a list of address pools for allocating addresses to remote clients, use the **address-pool** command in tunnel-group general-attributes configuration mode. To eliminate address pools, use the **no** form of this command.

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
interface name	(Optional) Specifies the interface to be used for the address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The address-pools settings in the group-policy **address-pools** command override the local pool settings in the tunnel group **address-pool** command.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in config-tunnel-general configuration mode, specifies a list of address pools for allocating addresses to remote clients for an IPSec remote-access tunnel group test:

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

address-pools (group-policy attributes configuration mode)

To specify a list of address pools for allocating addresses to remote clients, use the **address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
none	Specifies that no address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to 6 address pools from which to assign addresses.

Defaults

By default, the address pool attribute allows inheritance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The address-pools settings in this command override the local pool settings in the group. You can specify a list of up to six local address pools to use for local address allocation.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

The command **address-pools none** disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The command **no address pools none** removes the **address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example entered in config-general configuration mode, configures pool_1 and pool_20 as lists of address pools to use for allocating addresses to remote clients for GroupPolicy1:

```
hostname(config)# ip local pool pool_1 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool_20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool_1 pool_20
hostname(config-group-policy)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group-policies or for a particular group-policy.

admin-context

To set the admin context for the system configuration, use the **admin-context** command in global configuration mode. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the security appliance software or allowing remote management for an administrator), it uses one of the contexts that is designated as the admin context.

admin-context *name*

Syntax Description

name	Sets the name as a string up to 32 characters long. If you have not defined any contexts yet, then first specify the admin context name with this command. Then, the first context you add using the **context** command must be the specified admin context name. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.

Defaults

For a new security appliance in multiple context mode, the admin context is called "admin."

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

You cannot remove the current admin context, unless you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be "administrator":

```
hostname(config)# admin-context administrator
```

Related Commands

Command	Description
clear configure context	Removes all contexts from the system configuration.
context	Configures a context in the system configuration and enters context configuration mode.
show admin-context	shows the current admin context name.

alias

To manually translate an address and perform DNS reply modification, use the **alias** command in global configuration mode. To remove an **alias** command, use the **no** form of this command.

alias *interface_name mapped_ip real_ip* [*netmask*]

[no] alias *interface_name mapped_ip real_ip* [*netmask*]

Syntax Description

interface_name	Specifies the ingress interface name for traffic destined for the mapped IP address (or the egress interface name for traffic from the mapped IP address).
mapped_ip	Specifies the IP address to which you want to translate the real IP address.
netmask	(Optional) Specifies the subnet mask for both IP addresses. Enter **255.255.255.255** for a host mask.
real_ip	Specifies the real IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command functionality has been replaced by outside NAT commands, including the **nat** and **static** commands with the **dns** keyword. We recommend that you use outside NAT instead of the **alias** command.

Use this command to perform address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, use the **alias** command to redirect traffic to another address, such as 209.165.201.30.

Note If the **alias** command is used for DNS rewrite and not for other address translation, disable **proxy-arp** on the alias-enabled interface. Use the **sysopt noproxyarp** command to prevent the security appliance from pulling traffic toward itself via **proxy-arp** for generic NAT processing.

After changing or removing an **alias** command, use the **clear xlate** command.

An A (address) record must exist in the DNS zone file for the “dnat” address in the **alias** command.

The **alias** command has two uses that can be summarized in the following ways:

- If the security appliance gets a packet that is destined for the *mapped_ip*, you can configure the **alias** command to send it to the *real_ip*.
- If the security appliance gets a DNS packet that is returned to the security appliance destined for *real_ip*, you can configure the **alias** command to alter the DNS packet to change the destination network address to *mapped_ip*.

The **alias** command automatically interacts with the DNS servers on your network to ensure that domain name access to the aliased IP address is handled transparently.

Specify a net alias by using network addresses for the *real_ip* and *mapped_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

To access an **alias** *mapped_ip* address with **static** and **access-list** commands, specify the *mapped_ip* address in the **access-list** command as the address from which traffic is permitted as follows:

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

An alias is specified with the inside address 192.168.201.1 mapping to the destination address 209.165.201.1.

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client’s query would be altered by the security appliance to be 192.168.201.29. If the security appliance uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the security appliance with SRC=209.165.201.2 and DST=192.168.201.29. The security appliance translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

The following example shows that the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the security appliance because the client assumes that the 209.165.201.29 is on the local inside network. To correct this behavior, use the **alias** command as follows:

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

This example shows a web server that is on the inside at 10.1.1.11 and the **static** command that was created at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
dns-server# www.example.com. IN A 209.165.201.11
```

You must include the period at the end of the www.example.com. domain name.

This example shows how to use the **alias** command:

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

The security appliance changes the name server replies to 10.1.1.11 for inside clients to directly connect to the web server.

To provide access you also need the following commands:

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq
telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

Related Commands

Command	Description
access-list extended	Creates an access list.
clear configure alias	Removes all **alias** commands from the configuration.
show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.
static	Configures a one-to-one address translation rule by mapping a local IP address to a global IP address, or a local port to a global port.

allocate-interface

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. To remove an interface from a context, use the **no** form of this command.

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface***.***subinterface*[-*physical_interface***.***subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface***.***subinterface*[-*physical_interface***.***subinterface*]

Syntax Description

invisible	(Default) Allows context users to only see the mapped name (if configured) in the **show interface** command.

map_name	(Optional) Sets a mapped name.
	The *map_name* is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context.
	A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names:
	`int0`
	`inta`
	`int_0`
	For subinterfaces, you can specify a range of mapped names.
	See the "Usage Guidelines" section for more information about ranges.

physical_interface	Sets the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values. Do not include a space between the interface type and the port number.
subinterface	Sets the subinterface number. You can identify a range of subinterfaces.
visible	(Optional) Allows context users to see physical interface properties in the **show interface** command even if you set a mapped name.

Defaults

The interface ID is invisible in the **show interface** command output by default if you set a mapped name.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enter this command multiple times to specify different ranges. To change the mapped name or visible setting, reenter the command for a given interface ID, and set the new values; you do not need to enter the **no allocate-interface** command and start over. If you remove the **allocate-interface** command, the security appliance removes any interface-related configuration in the context.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA adaptive security appliance, you can use the dedicated management interface, Management 0/0, (either the physical interface or a subinterface) as a third interface for management traffic.

Note The management interface for transparent mode does not flood a packet out the interface when that packet is not in the MAC address table.

You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

  ```
  int0-int10
  ```

  If you enter **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**, for example, the command fails.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, both ranges include 100 interfaces:

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  If you enter **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**, for example, the command fails.

Examples

The following example shows gigabitethernet0/1.100, gigabitethernet0/1.200, and gigabitethernet0/2.300 through gigabitethernet0/1.305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN ID to a subinterface.

allocate-ips

To allocate an IPS virtual sensor to a security context if you have the AIP SSM installed, use the **allocate-ips** command in context configuration mode. To remove a virtual sensor from a context, use the **no** form of this command.

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

Syntax Description

default	(Optional) Sets one sensor per context as the default sensor; if the context configuration does not specify a sensor name, the context uses this default sensor. You can only configure one default sensor per context. If you want to change the default sensor, enter the **no allocate-ips** *sensor_name* command to remove the current default sensor before you allocate a new default sensor. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.
mapped_name	(Optional) Sets a mapped name as an alias for the sensor name that can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” senors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
sensor_name	Sets the sensor name configured on the AIP SSM. To view the sensors that are configured on the AIP SSM, enter **allocate-ips ?**. All available sensors are listed. You can also enter the **show ips** command. In the system execution space, the **show ips** command lists all available sensors; if you enter it in the context, it shows the sensors you already assigned to the context. If you specify a sensor name that does not yet exist on the AIP SSM, you get an error, but the **allocate-ips** command is entered as is. Until you create a sensor of that name on the AIP SSM, the context assumes the sensor is down.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM using the **ips** command, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts.

Note You do not need to be in multiple context mode to use virtual sensors; you can be in single mode and use different sensors for different traffic flows.

Examples

The following example assigns sensor1 and sensor2 to context A, and sensor1 and sensor3 to context B. Both contexts map the sensor names to "ips1" and "ips2." In context A, sensor1 is set as the default sensor, but in context B, no default is set so the default that is configured on the AIP SSM is used.

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
ips	Diverts traffic to the AIP SSM for inspection.
show context	Shows a list of contexts (system execution space) or information about the current context.
show ips	Shows the virtual sensors configured on the AIP SSM.

apcf

To enable an Application Profile Customization Framework profile, use the **apcf** command in webvpn configuration mode. To disable a particular APCF script, use the **no** version of the command. To disable all APCF scripts, use the **no** version of the command without arguments.

apcf URL/filename.ext

no apcf [URL/filename.ext]

Syntax Description

filename.extension	Specifies the name of the APCF customization script. These scripts are always in XML format. The extension might be .xml, .txt, .doc or one of many others
URL	Specifies the location of the APCF profile to load and use on the security appliance. Use one of the following URLs: http://, https://, tftp://, ftp://; flash:/, disk#:/' The URL might include a server, port, and path. If you provide only the filename, the default URL is flash:/. You can use the **copy** command to copy an APCF profile to flash memory.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **apcf** command enables the security appliance to handle non-standard web applications and web resources so that they render correctly over a WebVPN connection. An APCF profile contains a script that specifies when (pre, post), where (header, body, request, response), and what data to transform for a particular application.

You can use multiple APCF profiles on the security appliance. When you do, the security appliance applies each one of them in the order of oldest to newest.

We recommend that you use the apcf command only with the support of the Cisco TAC.

Examples

The following example shows how to enable an APCF named apcf1, located on flash memory at /apcf:

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

This example shows how to enable an APCF named apcf2.xml, located on an https server called myserver, port 1440 with the path being /apcf:

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

Related Commands

Command	Description
proxy-bypass	Configures minimal content rewriting for a particular application.
rewrite	Determines whether traffic travels through the security appliance.
show running config webvpn apcf	Displays the APCF configuration.

appl-acl

To identify a previously configured web-type ACL to apply to a session, use the **appl-acl** command in dap webvpn configuration mode. To remove the attribute from the configuration, use the **no** version of the command; to remove all web-type ACLs, use the **no** version of the command without arguments.

appl-acl *identifier*

no appl-acl [*identifier*]

Syntax Description

identifier	The name of the previously configured web-type ACL Maximum 240 characters.

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To configure web-type ACLs, use the **access-list_webtype** command in global configuration mode.

Use the **appl-acl** command multiple times to apply more than one web-type ACL to the DAP policy.

Examples

The following example shows how to apply the previously configured web-type ACL called newacl to the dynamic access policy:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# appl-acl newacl
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
access-list_webtype	Create web-type ACLs.

application-access

To customize the Application Access fiels of the WebVPN Home page that is displayed to authenticated WebVPN users, and the Application Access window that is launched when the user selects an application, use the **application-access** command from customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

no application-access {**title** | **message** | **window**} {**text** | **style**} *value*

Syntax Description

message	Changes the message displayed under the title of the Application Access field.
style	Changes the style of the Application Access field.
text	Changes the text of the Application Access field.
title	Changes the title of the Application Access field.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).
window	Changes the Application Access window.

Defaults

The default title text of the Application Access field is “Application Access”.

The default title style of the Application Access field is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text of the Application Access field is “Start Application Client”.

The default message style of the Application Access field is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default window text of the Application Access window is:

“Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications.”.

The default window style of the Application Access window is:

background-color:#99CCCC;color:black;font-weight:bold.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

This command is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command.

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

The following tips can help you make the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the Application Access field to the RGB hex value 66FFFF, a shade of green:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

Related Commands

Command	Description
application-access hide-details	Enable or disables the display of the application details in the Application Access window.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

application-access hide-details

To hide application details that are displayed in the WebVPN Applications Access window, use the **application-access hide-details** command from customization configuration mode, which is accessed by using the **webvpn** command or the **tunnel-group webvpn-attributes** command. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

application-access hide-details {**enable | disable**}

no application-access [**hide-details** {**enable | disable**}]

Syntax Description

disable	Does not hide application details in the Application Access window.
enable	Hides application details in the Application Access window.

Defaults

The default is disabled. Application details appear in the Application Access window.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example disables the appearance of the application details:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# application-access hide-details disable
```

Related Commands

Command	Description
application-access	Customizes the Application Access field of the WebVPN Home page.
browse-networks	Customizes the Browse Networks field of the WebVPN Home page.
web-applications	Customizes the Web Application field of the WebVPN Home page.

area

To create an OSPF area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

area *area_id*

no area *area_id*

Syntax Description

area_id	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The area that you create does not have any parameters set. Use the related area commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
hostname(config-router)# area 1
hostname(config-router)#
```

Related Commands

Command	Description
area authentication	Enables authentication for the OSPF area.
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area authentication

To enable authentication for an OSPF area, use the **area authentication** command in router configuration mode.

To disable area authentication, use the **no** form of this command.

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

Syntax Description

area_id	The identifier of the area on which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the *area_id*.

Defaults

Area authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified OSPF area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode. To restore the default cost value, use the **no** form of this command.

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost**

Syntax Description

area_id	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
cost	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535

Defaults

The default value of *cost* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in Type 3 LSAs between OSPF areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

Syntax Description

area_id	Identifier of the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
list_name	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only Type 3 LSAs can be filtered. If an ASBR is configured in the private network, then it will send Type 5 LSAs (describing private networks) which are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

Syntax Description

area_id	Identifier of the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric *metric_value*	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) the OSPF metric type for default routes. Valid values are the following: • **1**—type 1 • **2**—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Defaults

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

no area *area_id* **range** *address mask* [**advertise** | **not-advertise**]

Syntax Description

address	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates Type 3 summary link-state advertisements (LSAs).
area_id	Identifier of the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
mask	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The Type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Defaults

The address range status is set to advertise.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. Thus, OSPF can summarize addresses for many different sets of address ranges.

The **no area** *area_id* **range** *ip_address netmask* **not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode. To remove the stub area function, use the **no** form of this command.

area *area_id* [**no-summary**]

no area *area_id* [**no-summary**]

Syntax Description

area_id	Identifier for the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Defaults

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
authentication-key *key*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 *key*	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
router_id	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Defaults

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.

- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5** *key*: No key is predefined.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area** *area_id* **authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key** *key* or **message-digest-key** *key_id* **md5** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

To remove an option from a virtual link, use the **no** form of the command with the option that you want removed. To remove the virtual link, use the **no area** *area_id* **virtual-link** command.

Examples

The following example establishes a virtual link with MD5 authentication:

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command. A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the security appliance receives an ARP request for the specified IP address, then it responds with the security appliance MAC address. When the security appliance receives traffic destined for the host belonging to the IP address, the security appliance forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the security appliance does not perform proxy ARP.
interface_name	The interface attached to the host network.
ip_address	The host IP address.
mac_address	The host MAC address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver.

The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the security appliance, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the security appliance rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp timeout

To set the time before the security appliance rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

seconds	The number of seconds between ARP table rebuilds, from 60 to 4294967.

Defaults

The default value is 14,400 seconds (4 hours).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example changes the ARP timeout to 5,000 seconds:

```
hostname(config)# arp timeout 5000
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp timeout	Shows the current configuration of the ARP timeout.

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command. ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Defaults

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the security appliance. When you enable ARP inspection, the default is to flood non-matching ARP packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

- If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the security appliance, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the security appliance to drop any ARP packets that do not match the static ARP entry:

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

session	The session ID of the active ASDM session to be terminated. You can display the session IDs of all active ASDM sessions using the **show asdm sessions** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm disconnect** command to the **asdm disconnect** command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session	The session ID of the active ASDM logging session to be terminated. You can display the session IDs of all active ASDM sessions using the **show asdm log_sessions** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the security appliance. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, use the **asdm disconnect** command.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm group

Caution Do not manually configure this command. ASDM adds **asdm group** commands to the running configuration and uses them for internal purposes. This command is included in the documentation for informational purposes only.

asdm group *real_grp_name real_if_name*

asdm group *ref_grp_name ref_if_name* **reference** *real_grp_name*

Syntax Description

real_grp_name	The name of an ASDM object group.
real_if_name	The name of the interface to which the specified object group is associated.
ref_grp_name	The name of an object group that contains translated IP addresses of the object group specified by the *real_grp_name* argument.
ref_if_name	The name of the interface from which the destination IP address of inbound traffic is translated.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm group** command to the **asdm group** command.

Usage Guidelines

Do not manually configure or remove this command.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable

no asdm history enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm history enable** command to the **asdm history enable** command.

Usage Guidelines

The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples

The following example enables ASDM history tracking:

```
hostname(config)# asdm history enable
hostname(config)#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

asdm image

To specify the location of the ASDM software image in Flash memory, use the **asdm image** command in global configuration mode. To remove the image location, use the **no** form of this command.

asdm image *url*

no asdm image [*url*]

Syntax Description

url	Sets the location of the ASDM image in Flash memory. See the following URL syntax: • **disk0:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This URL indicates the internal Flash memory.

Defaults

If you do not include this command in your startup configuration, the security appliance uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external Flash memory. The security appliance then inserts the **asdm image** command into the running configuration if it discovered an image.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can store more than one ASDM software image in Flash memory. If you enter the **asdm image** command to specify a new ASDM software image while there are active ASDM sessions, the new command does not disrupt the active sessions; active ASDM sessions continue to use the ASDM

software image they started with. New ASDM sessions use the new software image. If you enter the **no asdm image** command, the command is removed from the configuration. However, you can still access ASDM from the security appliance using the last-configured image location.

If you do not include this command in your startup configuration, the security appliance uses the first ASDM image it finds at startup. It searches the root directory of internal Flash memory and then external Flash memory. The security appliance then inserts the **asdm image** command into the running configuration if it discovered an image. Be sure to save the running configuration to the startup configuration using the **write memory** command. If you do not save the **asdm image** command to the startup configuration, every time you reboot, the security appliance searches for an ASDM image and inserts the **asdm image** command into your running configuration. If you are using Auto Update, the automatic addition of this command at startup causes the configuration on the security appliance not to match the configuration on the Auto Update Server. This mismatch causes the security appliance to download the configuration from the Auto Update Server. To avoid unnecessary Auto Update activity, save the **asdm image** command to the startup configuration.

Examples

The following example sets the ASDM image to asdm.bin:

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.
boot	Sets the software image and startup configuration files.

asdm location

Caution Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

Syntax Description

ip_addr	IP address used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr*.
if_name	The name of the interface through which ASDM is accessed.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **pdm location** command to the **asdm location** command.

Usage Guidelines

Do not manually configure or remove this command.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*

no asr-group *group_id*

Syntax Description

group_id	The asymmetric routing group ID. Valid values are from 1 to 32.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	—	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When Active/Active failover is enabled, you may encounter situations where load balancing causes the return traffic for outbound connections to be routed through an active context on the peer unit, where the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be re-classified with the interface of the same asr-group if a flow with the incoming interface cannot be found. If re-classification finds a flow with another interface, and the associated context is in standby state, then the packet is forwarded to the active unit for processing.

Stateful Failover must be enabled for this command to take effect.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
hostname/ctx1(config)# interface Ethernet2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
hostname/ctx2(config)# interface Ethernet3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

assertion-consumer-url

To identify the URL that the security device accesses to contact the assertion consumer service, use the **assertion-consumer-url** command in the webvpn configuration mode for that specific SAML-type SSO server.

To remove the URL from the assertion, use the **no** form of this command.

assertion-consumer-url *url*

no assertion-consumer-url [*url*]

Syntax Description

url	Specifies the URL of the assertion consumer service used by the SAML-type SSO server. The URL must start with either http:// or https: and must be less than 255 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

If the URL begins with HTTPS, the requirement is to install the root certificate for the assertion consumer service's SSL certificate.

The following example specifies the assertion-consumer-url for a SAML-type SSO server:

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# assertion-consumer-url https://saml-server/postconsumer
hostname(config-webvpn-sso-saml#
```

Related Commands

Command	Description
issuer	Specifies the SAML-type SSO server security device name.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a WebVPN Single Sign-On server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

attribute

To specify attribute value pairs that the security appliance writes to the DAP attribute database, enter the **attribute** command in dap test attributes mode. Use this command multiple times to enter multiple attribute value pairs.

attribute *name value*

Syntax Description

name	Specifies a well-known attribute name, or an attribute that incorporates a "label" tag. The label tag corresponds to the Endpoint ID that you configure for file, registry, process, anti-virus, anti-spyware, and personal firewall endpoint attributes in the DAP record
value	The value assigned to the AAA attribute.

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
DAP attributes configuration mode	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Normally the security appliance retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The security appliance writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record.

Examples

The following example assumes that security appliance selects two DAP records if the authenticated user is a member of the SAP group and has anti-virus software installed on the endpoint system. The Endpoint ID for the anti-virus software endpoint rule is *nav*.

The DAP records have the following policy attributes:

DAP Record 1	DAP Record 2
action = continue	action = continue
port-forward = enable hostlist1	url-list = links2
	url-entry = enable

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)# attribute aaa.ldap.memberof SAP
hostname(config-dap-test-attr)# attribute endpoint.av.nav.exists true
hostname(config-dap-test-attr)# exit

hostname # test dynamic-access-policy execute
Policy Attributes:
action = continue
port-forward = enable hostlist1
url-list = links2
url-entry = enable

hostname #
```

Related CommandsI

Command	Description
display	Displays current attribute list.s
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes submode.
test dynamic-access-policy execute	Executes the logic that generates the DAP and displays the resulting access policies to the console.

auth-cookie-name

To specify the name of an authentication cookie, use the **auth-cookie-name** command in aaa-server host configuration mode. This is an SSO with HTTP Forms command.

auth-cookie-name

Syntax Description

name	The name of the authentication cookie. The maximum name size is 128 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. If authentication succeeds, the authenticating web server passes back an authentication cookie to the client browser. The client browser then authenticates to other web servers in the SSO domain by presenting the authentication cookie. The **auth-cookie-name** command configures name of the authentication cookie to be used for SSO by the security appliance.

A typical authentication cookie format is Set-Cookie: <cookie name>=<cookie value> [;<cookie attributes>]. In the following authentication cookie example, SMSESSION is the name that would be configured with the **auth-cookie-name** command:

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLDKTa8
ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw+MGiw0o8
8uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5d
c/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Pa
th=/
```

Examples

The following example specifies the authentication cookie name of SMSESSION for the authentication cookie received from a web server named example.com:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies that a username parameter must be submitted as part of the HTTP POST request used for SSO authentication.

authentication-certificate

To request a certificate from a WebVPN client establing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

Syntax Description

interface-name	The name of the interface used to establish the connection. Available interfaces names are: • **inside** Name of interface GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

- If you omit the **authentication-certificate** command, client certificate authentication is disabled.
- If you do not specify an interface-name with the **authentication-certificate** command, the default interface-name is **inside**

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections, however the ability to specify client certificate authentication for **management** connections with the **http authentication-certificate** command is available on all platforms, including the platforms that do not support WebVPN.

The security appliance validates certificates against the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the security appliance is not enabled.	The security appliance closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The security appliance redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the security appliance.
interface	Configures the interface used to establish the connection
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the ssl certificate trustpoint.

authentication-exclude

To enable end users to browse to configured links without logging in to clientless SSL VPN,, enter the **authentication-exclude** command in webvpn mode. Use this command multiple times to permit acccess to multiple sites.

authentication-exclude *url-fnmatch*

Syntax Description

url-fnmatch	Identifies the link to exempt from the requirement to log in to clientless SSL VPN.

Command Default

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This feature is useful when you require that some internal resources be available for public use via SSL VPN.

You need to distribute information about the links to end users in an SSL VPN-mangled form, for example, by browsing to these resources using SSL VPN and copying the resulting URLS into the information about links that you distribute.

Examples

The following example shows how to exempt two sites from authentication requirements:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-exclude http://www.site.com/public/*
hostname(config-webvpn)#authentication-exclude *announcement.html
hostname(config-webvpn)# hostname #
```

authentication

To configure the authentication method for WebVPN and e-mail proxies, use the **authentication** command in various modes. To restore the default method, use the **no** form of this command. The security appliance authenticates users to verify their identity.

authentication {[**aaa**] [**certificate**] [**mailhost**] [**piggyback]**}

no authentication [**aaa**] [**certificate**] [**mailhost**] [**piggyback]**

Syntax Description

aaa	Provides a username and password that the security appliance checks against a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server. For SMTPS only. For the IMAP4S and POP3S, mailhost authentication is mandatory and not displayed as a configurable option.
piggyback	Requires that an HTTPS WebVPN session already exists. Piggyback authentication is available for e-mail proxies only.

Defaults

The following table shows the default authentication methods for WebVPN and e-mail proxies:

Protocol	Default Authentication Method
IMAP4S	Mailhost (required)
POP3S	Mailhost (required)
SMTPS	AAA
WebVPN	AAA

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
SMTPS configuration	•	—	•	—	—
Webvpn configuration	•		•		

Command History

Release	Modification
8.0(2)	This command was introduced.

Release	Modification
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group webvpn-attributes configuration mode for WebVPN.
8.0(2)	This command was modified to reflect changes to certificate authentication requirements.

Usage Guidelines

At least one authentication method is required. For WebVPN, for example, you can specify AAA authentication, certificate authentication, or both. You can specify these in either order.

WebVPN certificate authentication requires that HTTPS user certificates be required for the respective interfaces. That is, for this selection to be operational, before you can specify certificate authentication, you must have specified the interface in an **authentication-certificate** command.

If you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group webvpn-attributes configuration mode.

For WebVPN, you can require both AAA and certificate authentication, in which case users must provide both a certificate and a username and password. For e-mail proxy authentication, you can require more than one authentication method. Specifying the command again overwrites the current configuration.

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

Related Commands

Command	Description
authentication-certificate	Requests a certificate from a WebVPN client establishing a connection.
show running-config	Displays the current tunnel-group configuration.
clear configure aaa	Remove/reset the configured AAA values.
show running-config aaa	Display the AAA configuration.

authentication eap-proxy

For L2TP over IPSec connections, to enable EAP and permit the security appliance to proxy the PPP authentication process to an external RADIUS authentication server, use the **authentication eap-proxy** command in tunnel-group ppp-attributes configuration mode. To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication eap-proxy

no authentication eap-proxy

Syntax Description

This command has no keywords or arguments.

Defaults

By default, EAP is not a permitted authentication protocol.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ppp-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Examples

The following example entered in config-ppp configuration mode, permits EAP for PPP connections for the tunnel group named ppremotegrp:

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication key eigrp

To enable authentication of EIGRP packets and specify the authentication key, use the **authentication key eigrp** command in interface configuration mode. To disable EIGRP authentication, use the **no** form of this command.

authentication key eigrp *as-number key* **key-id** *key-id*

no authentication key eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP process being authenticated. This must be the same values as configured for the EIGRP routing process.
key	Key to authenticate EIGRP updates. The key can contain up to 16 characters.
key-id *key-id*	Key identification value; valid values range from 1 to 255.

Defaults

EIGRP authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# authentication mode eigrp md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication mode eigrp	Specifies the type of authentication used for EIGRP authentication.

authentication mode eigrp

To specify the type of authentication used for EIGRP authentication, use the **authentication mode eigrp** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

authentication mode eigrp *as-num* **md5**

no authentication mode eigrp *as-num* **md5**

Syntax Description

as-num	The autonomous system number of the EIGRP routing process.
md5	Uses MD5 for EIGRP message authentication.

Defaults

No authentication is provided by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You must configure both the **authentication mode eigrp** and the **authentication key eigrp** commands on an interface to enable EIGRP message authentication. Use the **show running-config interface** command to view the **authentication** commands configured on an interface.

Examples

The following examples shows EIGRP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# authentication mode eigrp 100 md5
hostname(config-if)# authentication key eigrp 100 thisismykey key_id 5
```

Related Commands

Command	Description
authentication key eigrp	Enables authentication of EIGRP packets and specifies the authentication key.

authentication ms-chap-v1

For L2TP over IPSec connections, to enable Microsoft CHAP, Version 1 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode. This protocol is similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

To disable Microsoft CHAP, Version 1, use the **no** form of this command.

authentication ms-chap-v2

no authentication ms-chap-v2

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ppp-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

authentication ms-chap-v2

For L2TP over IPSec connections, to enable Microsoft CHAP, Version 2 authentication for PPP, use the **authentication ms-chap-v1** command in tunnel-group ppp-attributes configuration mode. This protocol is similar to CHAP but more secure in that the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. This protocol also generates a key for data encryption by MPPE.

To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

To disable Microsoft CHAP, Version 2, use the **no** form of this command.

authentication ms-chap-v1

no authentication ms-chap-v1

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ppp-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

authentication pap

For L2TP over IPSec connections, to permit PAP authentiation for PPP, use the **authentication pap** command in tunnel-group ppp-attributes configuration mode. This protocol passes cleartext username and password during authentication and is not secure.

To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication pap

no authentication pap

Syntax Description

This command has no keywords or arguments.

Defaults

By default, PAP is not a permitted authentication protocol.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ppp-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Examples

The following example entered in config-ppp configuration mode, permits PAP for PPP connections for a tunnel group named pppremotegrps:

```
hostname(config)# tunnel-group pppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authentication-certificate

To request a certificate from a WebVPN client establing a connection, use the **authentication-certificate** command in webvpn configuration mode. To cancel the requirement for a client certificate, use the **no** form of this command.

authentication-certificate *interface-name*

no authentication-certificate [*interface-name*]

Syntax Description

interface-name	The name of the interface used to establish the connection. Available interfaces names are: • **inside** Name of interface GigabitEthernet0/1 • **outside** Name of interface GigabitEthernet0/0

Defaults

- If you omit the **authentication-certificate** command, client certificate authentication is disabled.
- If you do not specify an interface-name with the **authentication-certificate** command, the default interface-name is **inside**

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For this command to take effect, WebVPN must already be enabled on the corresponding interface. An interface is configured and named with the **interface**, **IP address**, and **nameif** commands.

This command applies only to WebVPN client connections, however the ability to specify client certificate authentication for **management** connections with the **http authentication-certificate** command is available on all platforms, including the platforms that do not support WebVPN.

The security appliance validates certificates against the PKI trustpoints. If a certificate does not pass validation, then one of the following actions occurs:

If:	Then:
The local CA embedded in the security appliance is not enabled.	The security appliance closes the SSL connection.
The local CA is enabled, and AAA authentication is not enabled.	The security appliance redirects the client to the certificate enrollment page for the local CA to obtain a certificate.
Both the local CA and AAA authentication are enabled.	The client is redirected to a AAA authentication page. If configured, the client also is presented with a link to the enrollment page for the local CA.

Examples

The following example configures certificate authentication for WebVPN user connections on the outside interface:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-certificate outside
hostname(config-webvpn)#
```

Related Commands

Command	Description
authentication (tunnel-group webvpn configuration mode)	Specifies that the members of a tunnel group must use a digital certificate for authentication.
http authentication-certificate	Specifies authentication by means of certificate for ASDM management connections to the security appliance.
interface	Configures the interface used to establish the connection
show running-config ssl	Displays the current set of configured SSL commands.
ssl trust-point	Configures the ssl certificate trustpoint.

authentication-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-port** command in aaa-server configuration host configuration mode. To remove the authentication port specification, use the **no** form of this command. This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to assign authentication functions:

authentication-port *port*

no authentication-port

Syntax Description

port	A port number, in the range 1-65535, for RADIUS authentication.

Defaults

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number (1645) is used.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Semantic change to the command to support the specification of server ports on a per-host basis for server groups that contain RADIUS servers.

Usage Guidelines

If your RADIUS authentication server uses a port other than 1645, you must configure the security appliance for the appropriate port prior to starting the RADIUS service with the **aaa-server** command.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa authentication	Enables or disables LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication.
aaa-server host	Enters AAA server host configuration mode, so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

authentication-server-group (imap4s, pop3s, smtps)

To specify the set of authentication servers to use for e-mail proxies, use the **authentication-server-group** command in various modes. To remove authentication servers from the configuration, use the **no** form of this command. The security appliance authenticates users to verify their identity.

authentication-server-group *group_tag*

no authentication-server-group

Syntax Description

group_tag	Identifies the previously configured authentication server or group of servers. Use the **aaa-server** command to configure authentication servers.

Defaults

No authentication servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you configure AAA authentication, you must configure this attribute as well. Otherwise, authentication always fails.

Examples

The next example shows how to configure IMAP4S e-mail proxy to use the set of authentication servers named “IMAP4SSVRS”:

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.

authentication-server-group (tunnel-group general-attributes)

To specify the AAA server group to use for user authentication for a tunnel group, use the **authentication-server-group** command in tunnel-group general-attributes configuration mode. To return this attribute to the default, use the **no** form of this command.

authentication-server-group [(*interface_name*)] *server_group* [**LOCAL | NONE**]

no authentication-server-group [(*interface_name*)] *server_group*

Syntax Description

interface_name	(Optional) Specifies the interface where the IPSec tunnel terminates.
LOCAL	(Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either **LOCAL** or **NONE,** do not use the **LOCAL** keyword here.
NONE	(Optional) Specifies the server group name as **NONE**, indicating that authentication is not required.
server_group	Identifies the previously configured authentication server or group of servers.

Defaults

The default setting for the server-group in this command is **LOCAL**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
8.0(2)	This command was enhanced to allow per-interface authentication for IPSec connections.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Use the **aaa-server** command to configure authentication servers and the **aaa-server-host** command to add servers to a previously configured AAA server group.

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPSec remote-access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
aaa-server host	Adds servers to a previously configured AAA server group and configures host-specific AAA-server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.

authorization-dn-attributes

Note As of Release 8.0(4) this command has been deprecated. Use the **username-from-certificate** command in place of this command.

To specify the primary and secondary subject DN fields to use as the username for authorization, use the **authorization-dn-attributes** command in various configuration modes. To remove the attribute from the configuration and restore default values, use the **no** form of this command.

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no authorization-dn-attributes

Syntax Description

primary-attr	Specifies the attribute to use to derive a name for an authorization query from a certificate.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a name for an authorization query from a digital certificate.
use-entire-name	Specifies that the security appliance must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.

Defaults

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Added imap4s, pop3, and smtps configuration modes.

Usage Guidelines

Possible values for primary and secondary attributes include the following:

Attribute	Definition
CN	Common Name: the name of a person, system, or other entity
OU	Organizational Unit: the subgroup within the organization (O)
O	Organization: the name of the company, institution, agency, association or other entity
L	Locality: the city or town where the organization is located
SP	State/Province: the state or province where the organization is located
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
EA	E-mail address
T	Title
N	Name
GN	Given Name
SN	Surname
I	Initials
GENQ	Generational Qualifier
DNQ	Domain Name Qualifier
UID	User Identifier
UPN	User Principal Name
SER	Serial Number
use-entire-name	Use entire DN name

Examples

The following example, entered in global configuration mode, creates an IPSec remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute to use to derive a name for an authorization query from a digital certificate:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

authorization-required

To require users to authorize successfully prior to connecting, use the **authorization-required** command in various modes. To remove the attribute from the configuration, use the **no** version of this command.

authorization-required

no authorization-required

Syntax Description

This command has no arguments or keywords.

Defaults

Authorization-required is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.
7.2(1)	Replaced webvpn configuration mode with imap4s, pop3s, and smtps configuration modes.

Examples

The following example, entered in global configuration mode, requires authorization based on the complete DN for users connecting through a remote-access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPSec remote access) for the remote group named remotegrp. The second command enters tunnel-group general-attributes configuration mode for the specified tunnel group, and the last command specifies that authorization is required for the named tunnel group:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
authorization-dn-attributes	Specifies the primary and secondary subject DN fields to use as the username for authorization
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

authorization-server-group

To specify the set of authorization servers to use with WebVPN and e-mail proxies, use the **authorization-server-group** command in various modes. To remove authorization servers from the configuration, use the **no** form of this command. The security appliance uses authorization to verify the level of access to network resources that users are permitted.

authorization-server-group *group_tag*

no authorization-server-group

Syntax Description

group_tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.

Defaults

No authorization servers are configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

If you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

When VPN Authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example shows how to configure POP3S e-mail proxy to use the set of authorization servers named “POP3Spermit”:

```
hostname(config)# pop3s
```

```
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

The following example entered in config-general configuration mode, configures an authorization server group named “aaa-server78” for an IPSec remote-access tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

auth-prompt

To specify or change the AAA challenge text for through-the-security appliance user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, display the prompt *string*.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Defaults

If you do not specify an authentication prompt:

- FTP users see `FTP authentication`,
- HTTP users see `HTTP Authentication`
- Telnet users see no challenge text.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	Minor semantic changes.

Usage Guidelines

The **auth-prompt** command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the security appliance when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in.

If the user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the security appliance displays the **auth-prompt accept** text, if specified, to the user; otherwise it displays the **reject** text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

Note Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string "Please enter your username and password.":

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the security appliance accepts or rejects the authentication attempt; for example:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, "You're OK."

```
hostname(config)# auth-prompt accept You're OK.
```

After successfully authenticating, the user sees the following message:

```
You're OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-signon

To configure the security appliance to automatically pass user login credentials for Clientless SSL VPN connections on to internal servers, use the **auto-signon** command in any of three modes: webvpn configuration, webvpn group configuration, or webvpn username configuration mode. The authentication method can be NTLM (includes NTLMv1 and NTLMv2), HTTP Basic authentication, or both. To disable auto-signon to a particular server, use the **no** form of this command with the original **ip**, **uri**, and **auth-type** arguments. To disable auto-signon to all servers, use the **no** form of this command without arguments.

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}]

Syntax Description

all	Specifies both the NTLM and HTTP Basic authentication methods.
allow	Enables authentication to a particular server.
auth-type	Enables selection of an authentication method.
basic	Specifies the HTTP Basic authentication method.
ip	Specifies that an IP address and mask identifies the servers to be authenticated to.
ip-address	In conjunction with *ip-mask*, identifies the IP address range of the servers to be authenticated to.
ip-mask	In conjunction with *ip-address*, identifies the IP address range of the servers to be authenticated to.
ntlm	Specifies the NTLMv1 authentication method.
resource-mask	Identifies the URI mask of the servers to be authenticated to.
uri	Specifies that a URI mask identifies the servers to be authenticated to.

Defaults

By default, this feature is disabled for all servers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration (global)	•	—	•	—	—
Webvpn group policy configuration	•	—	•	—	—
Webvpn username configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(1)	NTLMv2 support was added. The **ntlm** keyword includes both NTLMv1 and NTLMv2.

Usage Guidelines

The **auto-signon** command is a single sign-on method for Clientless SSL VPN users. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, HTTP Basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).

You can use the auto-signon feature in three modes: webvpn configuration group-policy, webvpn configuration, or webvpn username configuration mode. The typical precedence behavior applies, where username supersedes group, and group supersedes global. The mode you choose depends upon the desired scope of authentication:

Mode	Scope
Webvpn configuration	All WebVPN users globally
Webvpn group configuration	A subset of WebVPN users defined by a group policy
Webvpn username configuration	An individual WebVPN user

Examples

The following example commands configure auto-signon for all Clientless users, using NTLM authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

The following example commands configure auto-signon for all Clientless users, using HTTP Basic authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

The following example commands configure auto-signon for Clientless users ExamplePolicy group policy, using either HTTP Basic or NTLM authentication, to servers defined by the URI mask https://*.example.com/*:

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type all
```

The following example commands configure auto-signon for a user named Anyuser, using HTTP Basic authentication, to servers with IP addresses ranging from 10.1.1.0 to 10.1.1.255:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type
basic
```

Related Commands

Command	Description
show running-config webvpn auto-signon	Displays auto-signon assignments of the running configuration.

auto-summary

To enable the automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in router configuration mode. To disable route summarization, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description

This command has no arguments or keywords.

Defaults

Route summarization is enabled for RIP Version 1, RIP Version 2, and EIGRP.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Support for EIGRP was added.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables.

RIP Version 1 always uses automatic summarization. You cannot disable automatic summarization for RIP Version 1.

If you are using RIP Version 2, you can turn off automatic summarization by specifying the **no auto-summary** command. Disable automatic summarization if you must perform routing between disconnected subnets. When automatic summarization is disabled, subnets are advertised.

EIGRP summary routes are given an administrative distance value of 5. You cannot configure this value.

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables RIP route summarization:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

The following example disables automatic EIGRP route summarization:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# no auto-summary
```

Related Commands

Command	Description
clear configure router	Clears all **router** commands and router configuration mode commands from the running configuration.
router eigrp	Enables the EIGRP routing process and enters EIGRP router configuration mode.
router rip	Enables the RIP routing process and enters RIP router configuration mode.
show running-config router	Displays the **router** commands and router configuration mode commands in the running configuration.

auto-update device-id

To configure the security appliance device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

Syntax Description

hardware-serial	Uses the hardware serial number of the security appliance to uniquely identify the device.
hostname	Uses the hostname of the security appliance to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the security appliance to uniquely identify the security appliance. By default, the security appliance uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name*.
mac-address [*if_name*]	Uses the MAC address of the security appliance to uniquely identify the security appliance. By default, the security appliance uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the *if_name*.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Defaults

The default ID is the hostname.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the device ID to the serial number:

```
hostname(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-at

To schedule a specific time for the security appliance to poll the Auto Update Server, use the **auto-update poll-at** command from global configuration mode. To remove all specified scheduling times for the security appliance to poll the Auto Update Server, use the **no** form of this command.

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

Syntax Description

days-of-the-week	Any single day or combination of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday. Other possible values are daily (Monday through Sunday), weekdays (Monday through Friday) and weekend (Saturday and Sunday).
randomize *minutes*	Specifies the period to randomize the poll time following the specified start time. from from 1 to 1439 minutes.
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait between connection attempts. The default is 5 minutes. The range is from 1 and 35791 minutes.
time	Specifies the time in the format HH:MM at which to start the poll. For example, 8:00 is 8:00 AM and 20:00 is 8:00 PM

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **auto-update poll-at** command specifys a time at which to poll for updates. If you enable the **randomize** option, the polling occurs at a random time within the range of the first *time* and the specified number of minutes. The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

In the following example, the security appliance polls the Auto Update Server every Friday and Saturday night at a random time between 10:00 p.m. and 11:00 p.m. If the security appliance is unable to contact the server, it tries two more times every 10 minutes.

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the security appliance.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the security appliance checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

poll_period	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Defaults

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **auto-update poll-at** and **auto-update poll-period** commands are mutually exclusive. Only one of them can be configured.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
hostname(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command. The security appliance periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

Syntax Description

interface	Specifies which interface to use when sending requests to the auto-update server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]**:**[[*user:password@*]*location* [:*port*]] / *pathname*
verify_certificate	Verifies the certificate returned by the Auto Update Server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The command was modified to add support for multiple servers.

Usage Guidelines

You can configure multiple servers to work with auto update. When checking for updates, a connection is made to the first server, but if that fails then the next server will be contacted. This will continue until all the servers have been tried. If all of them fail to connect, then a retry starting with the first server is attempted if the auto-update poll-period is configured to retry the connection.

For auto update functionality to work properly, you must use the **boot system configuration** command and ensure it specifies a valid boot image. Likewise, the **asdm image** command must be used with auto update to update the ASDM software image.

If the interface specified in the **source** *interface* argument is the same interface specified with the **management-access** command, requests to the auto-update server will be sent over the VPN tunnel.

Examples

The following example sets the Auto Update Server URL and specifies the interface outside:

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the security appliance.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. If the Auto Update Server has not been contacted for the timeout period, the security appliance stops all traffic through the security appliance. Set a timeout to ensure that the security appliance has the most recent image and configuration. To remove the timeout, use the **no** form of this command.

auto-update timeout *period*

no auto-update timeout [*period*]

Syntax Description

period	Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the **no** form of the command to reset it to 0.

Defaults

The default timeout is 0, which sets the security appliance to never time out.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A timeout condition is reported with system log message 201008.

Examples

The following example sets the timeout to 24 hours:

```
hostname(config)# auto-update timeout 1440
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.

clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

CHAPTER 4

backup interface through browse-networks Commands

backup interface

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **backup interface** command in interface configuration mode to identify a VLAN interface as a backup interface, for example, to an ISP. This command can be entered in the interface configuration mode for a VLAN interface only. This command blocks all through traffic on the identified backup interface unless the default route through the primary interface goes down. To restore normal operation, use the **no backup interface** command.

backup interface vlan *number*

no backup interface vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID of the backup interface.

Defaults

By default, the **backup interface** command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
7.2(2)	The Security Plus license no longer limits the number of VLAN interfaces to 3 for normal traffic, 1 for a backup interface, and 1 for failover; you can now configure up to 20 interfaces without any other limitations. Therefore the **backup interface** command is not required to enable more than 3 interfaces.

Usage Guidelines

When you configure Easy VPN with the **backup interface** command, if the backup interface becomes the primary, then the security appliance moves the VPN rules to the new primary interface. See the **show interface** command to view the state of the backup interface.

Be sure to configure default routes on both the primary and backup interfaces so that the backup interface can be used when the primary fails. For example, you can configure two default routes: one for the primary interface with a lower administrative distance, and one for the backup interface with a higher distance. See the **dhcp client route distance** command to override the administrative distance for default routes acquired from a DHCP server. To configure dual ISP support, see the **sla monitor** and **track rtr** commands for more information.

You cannot configure a backup interface when the **management-only** command is already configured on the interface.

Examples

The following example configures four VLAN interfaces. The backup-isp interface only allows through traffic when the primary interface is down. The **route** commands create default routes for the primary and backup interfaces, with the backup route at a lower administrative distance.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# backup interface vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# route outside 0 0 10.1.1.2 1
hostname(config)# route backup-isp 0 0 10.1.2.2 2
```

Related Commands

Command	Description
forward interface	Restricts an interface from initiating traffic to another interface.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
dhcp client route distance	Overrides the administrative distance for default routes acquired from a DHCP server.
sla monitor	Creates an SLA monitoring operation for static route tracking.
track rtr	Tracks the state of an SLA monitoring operation.

backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command. To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup-servers from another group policy.

IPSec backup servers let a VPN client connect to the central site when the primary security appliance is unavailable. When you configure backup servers, the security appliance pushes the server list to the client as the IPSec tunnel is established.

backup-servers {*server1 server2. . . . server10* **| clear-client-config | keep-client-config}**

no backup-servers [*server1 server2. . . . server10* **| clear-client-config | keep-client-config**]

Syntax Description

clear-client-config	Specifies that the client uses no backup servers. The security appliance pushes a null server list.
keep-client-config	Specifies that the security appliance sends no backup server information to the client. The client uses its own backup server list, if configured.
server1 server 2.... server10	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary security appliance is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

Defaults

Backup servers do not exist until you configure them, either on the client or on the primary security appliance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configure backup servers either on the client or on the primary security appliance. If you configure backup servers on the security appliance, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.

Examples

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

To configure the ASDM, session, login, or message-of-the-day banner, use the **banner** command in global configuration mode. The **no banner** command removes all lines from the banner keyword specified (**exec**, **login**, or **motd**).

banner {**asdm** | **exec | login | motd** *text*}

[no] banner {**asdm | exec | login | motd** [*text*]}

Syntax Description

asdm	Configures the system to display a banner after you successfully log in to ASDM. The user is prompted to either Continue to complete logging in, or to Disconnect. This option lets you require users to accept the terms of a written policy before connecting.
exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the security appliance using Telnet.
motd	Configures the system to display a message-of-the-day banner when you first connect.
text	Line of message text to display.

Defaults

The default is no banner.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.2(4)/8.0(3)	The **asdm** keyword was added.

Usage Guidelines

The **banner** command configures a banner to display for the keyword specified. The *text* string consists of all characters following the first white space (space) until the end of the line (carriage return or line feed [LF]). Spaces in the text are preserved. However, you cannot enter tabs through the CLI.

Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first.

Note The tokens $(domain) and $(hostname) are replaced with the hostname and domain name of the security appliance. When you enter a $(system) token in a context configuration, the context uses the banner configured in the system configuration.

Multiple lines in a banner are handled by entering a new banner command for each line that you wish to add. Each line is then appended to the end of the existing banner. There is no limit on the length of a banner other than RAM and Flash limits.

When accessing the security appliance through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs. Only the exec and motd banners support access to the security appliance through SSH. The login banner does not support SSH.

To replace a banner, use the **no banner** command before adding the new lines.

Use the **no banner** {**exec | login | motd**} command to remove all the lines for the banner keyword specified.

The **no banner** command does not selectively delete text strings, so any *text* that you enter at the end of the **no banner** command is ignored.

Examples

This example shows how to configure the **asdm**, **exec**, **login**, and **motd** banners:

```
hostname(config)# banner asdm You successfully logged in to ASDM
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
asdm:
You successfully logged in to ASDM

exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

This example shows how to add a second line to the **motd** banner:

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

Related Commands

Command	Description
clear configure banner	Removes all banners.
show running-config banner	Displays all banners.

banner (group-policy)

To display a banner, or welcome text, on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command. This option allows inheritance of a banner from another group policy. To prevent inheriting a banner, use the **banner none** command.

banner {**value** *banner_string* | **none}**

no banner

Note If you configure multiple banners under a VPN group-policy, and you delete any one of the banners, all banners will be deleted.

Syntax Description

none	Sets a banner with a null value, thereby disallowing a banner. Prevents inheriting a banner from a default or specified group policy.
value *banner_string*	Constitutes the banner text. Maximum string size is 500 characters. Use the "\n" sequence to insert a carriage return.

Defaults

There is no default banner.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to create a banner for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

blocks

To allocate additional memory to block diagnostics (displayed by the **show blocks** command), use the **blocks** command in privileged EXEC mode. To set the value back to the default, use the **no** form of this command. The amount of memory allocated will be at most 150 KB but never more than 50% of free memory. Optionally, you can specify the memory size manually.

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

Syntax Description

memory_size	(Optional) Sets the memory size for block diagnostics in bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message displays and the value is not accepted. If this value is greater than 50% of free memory, a warning message displays, but the value is accepted.

Defaults

The default memory assigned to track block diagnostics is 2136 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.

If you reload the security appliance, the memory allocation returns to the default.

Examples

The following example increases the memory size for block diagnostics:

```
hostname# blocks queue history enable
```

The following example increases the memory size to 3000 bytes:

```
hostname# blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 bytes, but the value is more than free memory:

```
hostname# blocks queue history enable 3000
```

```
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 bytes, but the value is more than 50% of free memory:

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

Command	Description
clear blocks	Clears the system buffer statistics.
show blocks	Shows the system buffer utilization.

boot

To specify which system image the system uses at the next reload and which configuration file the system uses at startup, use the **boot** command in global configuration mode. Use the **no** form of this command to restore the default value.

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

Syntax Description

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which system image file to use when the system is loaded.
url	Sets the location of the image or configuration. In multiple context mode, all remote URLs must be accessible from the admin context. See the following URL syntax: • **disk0:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This URL indicates the internal Flash memory. • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. This option is available for the **boot system** command for the ASA 5500 series adaptive security appliance only; the **boot config** command requires the startup configuration to be on the Flash memory. Only one **boot system tftp:** command can be configured, and it must be the first one configured.

Defaults

If the **boot config** command is not specified, the startup-config will be saved to a hidden location, and used only with commands that utilize it, such as the **show startup-config** command and the **copy startup-config** command.

For the **boot system** command, there are no defaults. If you do not specify a location, the security appliance searches only the internal Flash memory for the first valid image to boot. If no valid image is found, no system image will be loaded, and the security appliance will boot loop until ROMMON or Monitor mode is broken into.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you save this command to the startup configuration using the **write memory** command, you also save the settings to the BOOT and CONFIG_FILE environment variables, which the security appliance uses to determine the startup configuration and software image to boot when it restarts.

You can enter up to four **boot system** command entries, to specify different images to boot from in order, and the security appliance will boot the first valid image it finds.

If you want to use a startup configuration file at the new location that is different from the current running configuration, then be sure to copy the startup configuration file to the new location after you save the running configuration. Otherwise, the running configuration will overwrite the new startup configuration when you save it.

Tip The ASDM image file is specified by the **asdm image** command.

Examples

The following example specifies that at startup the security appliance should load a configuration file called configuration.txt:

```
hostname(config)# boot config disk0:/configuration.txt
```

Related Commands

Command	Description
asdm image	Specifies the ASDM software image.
show bootvar	Displays boot file and configuration environment variables.

border style

To customize the border of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **border style** command from customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

border style *value*

no border style *value*

Syntax Description

value	The Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default style of the border is background-color:#669999;color:white.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the background color of the border to the RGB color #66FFFF, a shade of green:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# border style background-color:66FFFF
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

browse-networks

To customize the Browse Networks box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **browse-networks** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

no browse-networks [{**title** | **message** | **dropdown**} {**text** | **style**} *value*]

Syntax Description

dropdown	Specifies you are changing the drop-down list.
message	Specifies you are changing the message displayed under the title.
style	Specifies you are changing the style.
text	Specifies you are changing the text.
title	Specifies you are changing the title.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is “Browse Networks”.

The default title style is:

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

The default message text is “Enter Network Path”.

The default message style is:

background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “File Folder Bookmarks”.

The default dropdown style is:

border:1px solid black;font-weight:bold;color:black;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the title to “Browse Corporate Networks”, and the text within the style to blue:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
F1-asa1(config-webvpn-custom)# browse-networks title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

CHAPTER 5

cache through clear compression Commands

cache

To enter cache mode and set values for caching attributes, enter the **cache** command in webvpn configuration mode. To remove all cache related commands from the configuration and reset them to their default values, enter the **no** version of this command.

cache

no cache

Defaults

Enabled with default settings for each cache attribute.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to enter cache mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache-static-content	Caches content not subject to rewriting.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

cache-fs limit

To limit the size of the cache file system used to store images that the security appliance downloads to remote PCs, use the **cache-fs limit** command from webvpn configuration mode. Use the **no** form of this commandto return to the default value.

cache-fs limit {*size*}

no cache-fs limit {*size*}

Syntax Description

size	Size limit of the cache file system, from 1 to 32 MB.

Defaults

The default value is 20 MB.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance expands package files containing images and files for the Cisco AnyConnect VPN Client and Cisco Secure Desktop (CSD) in cache memory for downloading to remote PCs. For the security appliance to successfully expand the package files, there must be enough cache memory to store the images and files.

If the security appliance detects there is not enough cache memory to expand a package, it displays an error message to the console. The following example shows an error message reported after an attempt to install an AnyConnect VPN Client image package with the **svc image** command:

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

If this occurs when you attempt to install an image package, you can examine the amount of cache memory remaining and the size of any previously installed packages with the **dir cache:/** command from global configuration mode. Then you can adjust the cache size limit accordingly.

Examples

The following example indicates the CSD image (located in sdesktop) and the CVC image (located in stc) use approximately 5.44 MB of cache memory:

```
hostname(config-webvpn)# dir cache:/
```

```
Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)
```

The next example limits the cache size to 6 MB:

```
hostname(config-webvpn)# cache-fs limit 6
```

Related Commands

Command	Description
dir cache:/	Displays the contents of cache memory, including the total cache memory reserved and the remaining amount of cache memory.
show run webvpn	Displays the current WebVPN configuration, including any SSL VPN client or CSD images installed that may consume cache memory.
show webvpn csd	Displays the CSD version and installation status.
show webvpn svc	Displays the name and versions of installed SSL VPN package files.

cache-static-content

To configure the security appliance to load all static content used for clientless SSL VPN connections in cache memory, use the **cache-static-content** command from webvpn cache configuration mode.

cache-static-content enable

no cache-static-content enable

Syntax Description

enable	Enables the loading of all static content into cache memory.

Defaults

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn cache configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Configuring the security appliance to store all cacheable static content in the security appliance cache increases the performance of backend SSL VPN connections. Static content includes objects not rewritten (mangled) by the security appliance, such as PDF files and images.

Examples

The following example enabled caching of static content:

```
hostname(config-webvpn-cache)# cache-static-content enable
```

Related Commands

Command	Description
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.

cache-time

To specify in minutes how long to allow a CRL to remain in the cache before considering it stale, use the **cache-time** command in crl configure configuration mode, which is accessible from crypt ca trustpoint configuration mode. To return to the default value, use the **no** form of this command.

cache-time *refresh-time*

no cache-time

Syntax Description

refresh-time	Specifies the number of minutes to allow a CRL to remain in the cache. The range is 1 - 1440 minutes. If the NextUpdate field is not present in the CRL, the CRL is not cached.

Defaults

The default setting is 60 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and specifies a cache time refresh value of 10 minutes for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
enforcenextupdate	Specifies how to handle the NextUpdate CRL field in a certificate.

call-agent

To specify a group of call agents, use the **call-agent** command in MGCP map configuration mode, which is accessible by using the **mgcp-map** command. To remove the configuration, use the **no** form of this command.

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

Syntax Description

ip_address	The IP address of the gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **call-agent** command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. Call agents with the same *group_id* belong to the same group. A call agent may belong to more than one group. The *group_id* option is a number from 0 to 4294967295. The *ip_address* option specifies the IP address of the call agent.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
```

```
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

call-duration-limit

To configure the call duration for an H.323 call, use the **call-duration-limit** command in parameters configuration mode, which is accessible from policy-map configuration mode. To disable this feature, use the **no** form of this command.

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

Syntax Description

hh:mm:ss	Specifies the duration in hours, minutes, and seconds.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure the call duration for an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-duration-limit 0:1:0
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

call-party-numbers

To enforce sending call party numbers during an H.323 call setup, use the **call-party-numbers** command in parameters configuration mode, which is accessible from policy-map configuration mode. To disable this feature, use the **no** form of this command.

call-party-numbers

no call-party-numbers

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enforce call party numbers during call setup for an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-party-numbers
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command in privileged EXEC mode. To disable packet capture capabilities, use the **no** form of this command.

capture *capture_name* [**type** {**asp-drop all** [*drop-code*] | **raw-data** | **isakmp** | **decrypted** | **webvpn user** *webvpn-user* [**url** *url*]}] [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

no capture *capture-name* [**type** {**asp-drop** [*drop-code*] | **raw-data** | **isakmp** | **decrypted | webvpn user** *webvpn-user***]** [**access-list** *access_list_name*] [**circular-buffer**] [**interface** *interface_name*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot*] {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

Syntax Description

access-list *access_list_name*	(Optional) Captures traffic that matches an access list. In multiple context mode, this is only available within a context.
any	Specifies any IP address instead of a single IP address and mask.
all	Captures all the packets that the security appliance drops
asp-drop [*drop-code***]**	(Optional) Captures packets dropped by the accelerated security path. The *drop-code* specifies the type of traffic that is dropped by the accelerated security path. See the **show asp drop frame** command for a list of drop codes. If you do not enter the *drop-code* argument, then all dropped packets are captured. You can enter this keyword with **packet-length**, **circular-buffer**, and **buffer**, but not with **interface** or **ethernet-type**.
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops.
capture_name	Specifies the name of the packet capture. Use the same name on multiple **capture** statements to capture multiple types of traffic. When you view the capture configuration using the **show capture** command, all options are combined on one line.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link transport.
decrypted	(Optional) Decrypted TCP data is encapsulated with L2-L4 headers, and captured by the capture engine.
ethernet-type *type*	(Optional) Selects an Ethernet type to capture. The default is IP packets. An exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching.
host *ip*	Specifies the single IP address of the host to which the packet is being sent.

interface *interface_name*	Sets the name of the interface on which to use packet capture. You must configure an interface for any packets to be captured. You can configure multiple interfaces using multiple **capture** commands with the same name. To capture packets on the dataplane of an ASA 5500 series adaptive security appliance, you can use the **interface** keyword with **asa_dataplane** as the name of the interface.
isakmp	(Optional) Captures ISAKMP traffic. This is not available in multiple context mode. The ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the Physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.
mask	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The security appliance uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
match *prot*	Specifies the packets that match the five-tuple to allow filtering of those packets to be captured. You can use this keyword up to three times on one line.
operator	(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows: • **lt**—less than • **gt**—greater than • **eq**—equal to
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
port	(Optional) If you set the protocol to **tcp** or **udp**, specifies the integer or name of a TCP or UDP port.
raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces. This setting is the default.
real-time	Displays the captured packets continuously in real-time. To terminate real-time packet capture, enter **Ctrl + c.** This option applies only to **raw-data** and **asp-drop** captures.
trace *trace_count*	(Optional) Captures packet trace information, and the number of packets to capture. This is used with an access list to insert trace packets into the data path to determine whether the packet is processed as expected.
type	(Optional) Specifies the type of data captured.
url *url*	(Optional) Specifies a URL prefix to match for data capture. Use the URL format http://*server*/*path* to capture HTTP traffic to the server. Use https://*server*/*path* to capture HTTPS traffic to the server.
user *webvpn-user*	(Optional) Specifies a username for a WebVPN capture.
webvpn	(Optional) Captures WebVPN data for a specific WebVPN connection.

Defaults

The defaults are as follows:

- The default **type** is **raw-data**.
- The default **buffer** *size* is 512 KB.
- The default Ethernet type is IP.
- The default **packet-length** is 1518 bytes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Priveleged EXEC	•	•	•	•	•

Command History

Release	Modification
6.2(1)	This command was introduced.
7.0(1)	This command was modified to include the following keywords: **type asp-drop**, **type isakmp**, **type raw-data**, and **type webvpn**.
7.0(8)	Added the **all** option to capture all packets that the security appliance drops**.**
7.2(1)	This command was modified to include the following options: **trace** *trace_count*, **match** *prot*, **real-time, host** *ip*, **any**, *mask*, and *operator.*
8.0(2)	This command was modified to update the path to capture contents.
8.0(4)	This command was modified to include the following keyword: **type decrypted**.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. You can create multiple captures. To view the packet capture, use the **show capture** *name* command. To save the capture to a file, use the **copy capture** command. Use the **https://***security appliance-ip-address*/*admin*/**capture**/*capture_name*[/**pcap**] command to see the packet capture information with a web browser. If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

Note Enabling WebVPN capture affects the performance of the security appliance. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** keyword is specified, the capture is detached from the specified interface and the capture is preserved. Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself.

You cannot perform any operations on a capture while the real-time display is in progress. Using the **real-time** keyword with a slow console connection may result in an excessive number of non-displayed packets because of performance considerations. The fixed limit of the buffer is 1000 packets. If the buffer fills up, a counter is maintained of the captured packets. If you open another session, you can disable the real-time display be entering the **no capture real-time** command.

Note The **capture** command is not saved to the configuration, and is not copied to the standby unit during failover.

Examples

To capture a packet, enter the following command:

```
hostname# capture captest interface inside
hostname# capture captest interface outside
```

On a web browser, the contents of the capture command that was issued, named "captest", can be viewed at the following location:

```
https://171.69.38.95/admin/capture/captest
```

To download a libpcap file (which web browsers use) to a local machine, enter the following command:

```
https://171.69.38.95/capture/http/pcap
```

The following example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
hostname# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname# capture http access-list http packet-length 74 interface inside
```

The following example shows how to capture ARP packets:

```
hostname# capture arp ethernet-type arp interface outside
```

The following example inserts five tracer packets into the data stream, where *access-list 101* defines traffic that matches TCP protocol FTP :

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

To view the traced packets and information about packet processing in an easily readable manner, use the **show capture ftptrace** command.

This example shows how to display captured packets in real-time:

```
hostname# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

Related Commands

Command	Description
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.
show capture	Displays the capture configuration when no options are specified.

cd

To change the current working directory to the one specified, use the **cd** command in privileged EXEC mode.

cd [**disk0: | disk1: | flash:]** [*path*]

Syntax Description

disk0*:*	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the removable, external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
path	(Optional) The absolute path of the directory to change to.

Defaults

If you do not specify a directory, the directory is changed to the root directory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to change to the “config” directory:

```
hostname# cd flash:/config/
```

Related Commands

Command	Description
pwd	Displays the current working directory.

cdp-url

To specify the CDP to be included in certificates issued by the local CA, use the **cdp-url** command in CA server configuration mode. To revert to the default CDP, use the **no** form of this command.

[no] cdp-url *url*

Syntax Description

url	Specifies the URL where a validating party obtains revocation status for certificates issued by the local CA. The URL must be less than 500 alphanumeric characters.

Defaults

The default CDP URL is that of the security appliance that includes the local CA. The default URL is in the format: http://hostname.domain/+CSCOCA+/asa_ca.crl

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The CDP is an extension that can be included in issued certificates to specify the location where a validating party can obtain revocation status for the certificate. Only one CDP can be configured at a time.

Note If a CDP URL is specified, it is the responsibility of the administrator to maintain access to the current CRL from that location.

Examples

The following example configures a CDP at 10.10.10.12 for certificates issued by the local CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by a local CA server as revoked in the certificate database and CRL.
crypto ca server unrevoke	Unrevokes a previously revoked certificate issued by a local CA server.
lifetime crl	Specifies the lifetime of the certificate revocation list.

certificate

Use the **certificate** command in crypto ca certificate chain configuration mode to add the indicated certificate. Whenthis command is issued, the security appliance interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate. To delete the certificate, use the **no** form of this command.

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number	Specifies the serial number of the certificate in hexadecimal format ending with the word quit.
ca	Indicates that the certificate is a CA issuing certificate.
ra-encrypt	Indicates that the certificate is an RA key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is an RA certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an RA digital signature certificate used in SCEP messaging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca certificate chain configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A CA is an authority in a network that issues and manages security credentials and public key for message encryption. As part of a public key infrastructure, a CA checks with a RA to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor information, the CA can then issue a certificate.

Examples

The following example adds a CA certificate with a serial number 29573D5FF010FE25B45:

```
hostname(config)# crypto ca trustpoint central
```

```
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
crypto ca certificate chain	Enters certificate crypto ca certificate chain mode.
crypto ca trustpoint	Enters ca trustpoint mode.
show running-config crypto map	Displays all configuration for all the crypto maps.

certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel-group map associations, use the **no** form of this command.

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

Syntax Description

certificate_map_name	The name of a certificate map.
index	The numeric identifier for a map entry in the certificate map. The index value can be in a range of 1-65535.
tunnel_group_name	the name of the tunnel group chosen if the map entry matches the certificate. The *tunnel-group name* must already exist.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

With the **certificate-group-map** command in effect, if a certificate received from a WebVPN client corresponds to a map entry, the resulting tunnel-group is associated with the connection, overriding any tunnel-group choice made by the user.

Multiple instances of the **certificate-group-map** command allow multiple mappings.

Examples

The following example shows how to associate rule 6 for a tunnel-group named tgl:

```
hostname(config)# webvpn
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map configuration mode for configuring rules based on the certificate's issuer and subject distinguished names (DNs).
tunnel-group-map	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

chain

To enable sending of a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. This action includes the root certificate and any subordinate CA certificates in the transmission. To return this command to the default, use the **no** form of this command.

chain

no chain

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPSec tunnel-group types.

Examples

The following example entered in tunnel-group-ipsec attributes configuration mode, enables sending a chain for an IPSec LAN-to-LAN tunnel group with the IP address of 209.165.200.225, which includes the root certificate and any subordinate CA certificates:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the current tunnel-group configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto {**system** | **context** *name*}

Syntax Description

context *name*	Changes to the context with the specified name.
system	Changes to the system execution space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you log into the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. The "running" configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on which execution space you are in. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context execution space, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration appears.

Examples

The following example changes between contexts and the system in privileged EXEC mode:

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

The following example changes between the system and the admin context in interface configuration mode. When you change between execution spaces, and you are in a configuration submode, the mode changes to the global configuration mode in the new execution space.

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

Related Commands

Command	Description
admin-context	Sets a context to be the admin context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

character-encoding

To specify the global character encoding in WebVPN portal pages, use the **character-encoding** command in webvpn configuration mode. To remove the value of the character-encoding attribute, use the **no** form of this command.

character-encoding *charset*

no character-encoding [*charset***]**

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper-case to lower-case in the security appliance configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0’s and 1’s) and characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly. The character-encoding attribute lets the user specify the value of the character-encoding method into the WebVPN portal page to ensure that the browser renders it properly, regardless of the region in which the user is using the browser, or any changes made to the browser.

The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, the user can override the file-encoding attribute for Common Internet File System servers that use character encoding that differs from the value of the character-encoding attribute. Use different file-encoding values for CIFS servers that require different character encodings.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character-encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. The user needs to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

The encoding type set on the remote browser determines the character set for WebVPN portal pages when this attribute does not have a value.

Examples

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

Related Commands

Command	Description
file-encoding	Specifies CIFS servers and associated character encoding to override the value of this attribute.
show running-config [all] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debug messages about the CIFS.

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

checkheaps {check-interval | **validate-checksum}** *seconds*

no checkheaps {check-interval | **validate-checksum}** [*seconds*]

Syntax Description

check-interval	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the security appliance checks the entire heap, validating each memory buffer. If there is a discrepancy, the security appliance issues either an “allocated buffer error” or a “free buffer error.” If there is an error, the security appliance dumps traceback information when possible and reloads.
validate-checksum	Sets the code space checksum validation interval. When the security appliance first boots up, the security appliance calculates a hash of the entire code. Later, during the periodic check, the security appliance generates a new hash and compares it to the original. If there is a mismatch, the security appliance issues a “text checksum checkheaps error.” If there is an error, the security appliance dumps traceback information when possible and reloads.
seconds	Sets the interval in seconds between 1 and 2147483.

Defaults

The default intervals are 60 seconds each.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

Related Commands

Command	Description
show checkheaps	Shows checkheaps statistics.

check-retransmission

To prevent against TCP retransmission style attacks, use the **check-retransmission** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

check-retransmission

no check-retransmission

Syntax Description

This command has no arguments or keywords.

Defaults

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. To prevent against TCP retransmission style attacks that arise from end-system interpretation of inconsistent retransmissions, use the **check-retransmission** command in tcp-map configuration mode.

The security appliance will make efforts to verify if the data in retransmits are the same as the original. If the data does not match, then the connection is dropped by the security appliance. When this feature is enabled, packets on the TCP connection are only allowed in order. For more details, see the **queue-limit** command.

Examples

The following example enables the TCP check-retransmission feature on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification

no checksum-verification

Syntax Description

This command has no arguments or keywords.

Defaults

Checksum verification is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap

hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

cipc security-mode authenticated

To force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario, use the **cipc security-mode authenticated** command in phone-proxy configuration mode.

To turn off this command when CIPC softphones support encryption, use the **no** form of this command.

cipc security-mode authenticated

no cipc security-mode authenticated

Syntax Description

There are no arguments for keywords for this command.

Defaults

Be default, this command is disabled via the no form of the command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Separating voice and data traffic by using VLANs is a security best practice to hide voice streams from security threats that attempt to penetrate the data VLAN. However, Cisco IP Communicator (CIPC) softphone applications must connect to their respective IP phones, which reside on the voice VLAN. This requirement makes segregating voice and data VLANs an issue because the SIP and SCCP protocols dynamically negotiate the RTP/RTCP ports on a wide range of ports. This dynamic negotiation requires that a range of ports be open between the two VLANs.

Note Earlier versions of CIPC that do not support Authenticated mode are not supported with the Phone Proxy.

To allow CIPC softphones on the data VLAN to connect to their respective IP phones on the voice VLAN without requiring access between the VLANs on a wide range of ports, you can configure the Phone Proxy with the **cipc security-mode authenticated** command.

This command allows the Phone Proxy to look for CIPC configuration files and force CIPC softphones to be in authenticated mode rather than encrypted mode because current versions of CIPC do not support encrypted mode.

When this command is enabled, the Phone Proxy parses the phones configuration file to determine if the phone is a CIPC softphone and changes the security mode to authenticated. Additionally, CIPC softphones support authenticated mode only while the Phone Proxy, by default, forces all phones to be in encrypted mode.

Examples

The following example shows the use of the **cipc security-mode authenticated** command to force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)#cipc security-mode authenticated
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

class (global)

To create a resource class to which to assign a security context, use the **class** command in global configuration mode. To remove a class, use the **no** form of this command.

class *name*

no class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To set the limits for the default class, enter **default** for the name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the security appliance, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

The security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

When you create a class, the security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the security appliance sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can “use up” those resources, potentially affecting service to other contexts. See the **limit-resource** command to set the resources for the class.

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all

concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with limits for all resources, the class uses no settings from the default class.

By default, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- MAC addresses—65,535 entries.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

Related Commands

Command	Description
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.
show class	Shows the contexts assigned to a class.

class (policy-map)

To assign a class map to a policy map where you can assign actions to the class map traffic, use the **class** command in policy-map configuration mode. To remove a class map from a policy map, use the **no** form of this command.

class *classmap_name*

no class *classmap_name*

Syntax Description

classmap_name	Specifies the name for the class map. For a Layer 3/4 policy map (the **policy-map** command), you must specify a Layer 3/4 class map name (the **class-map** or **class-map type management** command). For an inspection policy map (the **policy-map type inspect** command), you must specify an inspection class map name (the **class-map type inspect** command).

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To use the **class** command, use the Modular Policy Framework. To use a class in a Layer 3/4 policy map, enter the following commands:

1. **class-map**—Identify the traffic on which you want to perform actions.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features*—For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more details about the commands available for each feature.
3. **service-policy**—Assigns the policy map to an interface or globally.

To use a class in an inspection policy map, enter the following commands:

1. **class-map type inspect**—Identify the traffic on which you want to perform actions.
2. **policy-map type inspect**—Identify the actions associated with each class map.
   a. **class**—Identify the inspection class map on which you want to perform actions.
   b. *commands for application types*—See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for commands available for each application type. Actions supported in class configuration mode of an inspection policy map include:
   - Dropping a packet
   - Dropping a connection
   - Resetting a connection
   - Logging
   - Rate-limiting of messages
   - Masking content

   c. **parameters**—Configure parameters that affect the inspection engine. The CLI enters parameters configuration mode. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for available commands.
3. **class-map**—Identify the traffic on which you want to perform actions.
4. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the Layer 3/4 class map on which you want to perform actions.
   b. **inspect** *application inspect_policy_map*—Enables application inspection, and calls an inspection policy map to perform special actions.
5. **service-policy**—Assigns the policy map to an interface or globally.

The configuration always includes a class map called **class-default** that matches all traffic. At the end of every Layer 3/4 policy map, the configuration includes the **class-default** class map with no actions defined. You can optionally use this class map when you want to match all traffic, and do not want to bother creating another class map. In fact, some features are only configurable for the **class-default** class map, such as the **shape** command.

Including the **class-default** class map, up to 63 **class** and **match** commands can be configured in a policy map.

Examples

The following is an example of a **policy-map** command for connection policy that includes the **class** command. It limits the number of connections allowed to the web server 10.1.1.1:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
```

```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the security appliance does not make this match because they previously matched other classes.

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
class-map type management	Creates a Layer 3/4 class map for management traffic.
clear configure policy-map	Removes all policy-map configuration, except for any policy-map that is in use in a service-policy command.
match	Defines the traffic-matching parameters.
policy-map	Configures a policy; that is, an association of one or more traffic classes, each with one or more actions.

class-map

When using the Modular Policy Framework, identify Layer 3 or 4 traffic to which you want to apply actions by using the **class-map** command (without the **type** keyword) in global configuration mode. To delete a class map, use the **no** form of this command.

class-map *class_map_name*

no class-map *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This type of class map is for Layer 3/4 through traffic only. For management traffic destined to the security appliance, see the **class-map type management** command.

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. You can create multiple Layer 3/4 class maps for each Layer 3/4 policy map.

Default Class Maps

The configuration includes a default Layer 3/4 class map that the security appliance uses in the default global policy. It is called **inspection_default** and matches the default inspection traffic:

```
class-map inspection_default
 match default-inspection-traffic
```

Another class map that exists in the default configuration is called class-default, and it matches all traffic:

```
class-map class-default
 match any
```

This class map appears at the end of all Layer 3/4 policy maps and essentially tells the security appliance to not perform any actions on all other traffic. You can use the class-default class map if desired, rather than making your own **match any** class map. In fact, some features are only available for class-default, such as QoS traffic shaping.

Maximum Class Maps

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types.

Configuration Overview

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Use the **class-map** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. A Layer 3/4 class map contains, at most, one **match** command (with the exception of the **match tunnel-group** and **match default-inspection-traffic** commands) that identifies the traffic included in the class map.

Examples

The following example creates four Layer 3/4 class maps:

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

Related Commands

Command	Description
class-map type management	Creates a class map for traffic to the security appliance.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type inspect

When using the Modular Policy Framework, match criteria that is specific to an inspection application by using the **class-map type inspect** command in global configuration mode. To delete an inspection class map, use the **no** form of this command.

class-map type inspect *application* [**match-all** | **match-any]** *class_map_name*

no class-map [**type inspect** *application* [**match-all** | **match-any**]] *class_map_name*

Syntax Description

application	Specifies the type of application traffic you want to match. Available types include: • **dns** • **ftp** • **h323** • **http** • **im** • **sip**
class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-all	(Optional) Specifies that traffic must match all criteria to match the class map. **match-all** is the default if you do not specify an option.
match-any	(Optional) Specifies that traffic can match one or more criteria to match the class map.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	The **match-any** keyword was added.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map. The class map contains one or more **match** commands. (You can alternatively use **match** commands directly in the inspection policy map if you want to pair a single criterion with an action). You can match criteria that is specific to an application. For example, for DNS traffic, you can match the domain name in a DNS query.

A class map groups multiple traffic matches (in a match-all class map), or lets you match any of a list of matches (in a match-any class map). The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you group multiple match commands, and you can reuse class maps. For the traffic that you identify in this class map, you can specify actions such as dropping, resetting, and/or logging the connection in the inspection policy map.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates an HTTP class map that must match all criteria:

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

The following example creates an HTTP class map that can match any of the criteria:

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map for through traffic.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type management

When using the Modular Policy Framework, identify Layer 3 or 4 management traffic destined for the security appliance to which you want to apply actions by using the **class-map type management** command in global configuration mode. To delete a class map, use the **no** form of this command.

class-map type management *class_map_name*

no class-map type management *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	The s**et connection** command is now available for a Layer 3/4 management class map, for to-the-security appliance management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.

Usage Guidelines

This type of class map is for management traffic only. For through traffic, see the **class-map** command (without the **type** keyword).

For management traffic to the security appliance, you might want to perform actions specific to this kind of traffic. The types of actions available for a management class map in the policy map are specialized for management traffic. For example, this type of class map lets you inspect RADIUS accounting traffic and set connection limits.

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. The maximum number of class maps of all types is 255 in single mode or per context in multiple mode.

You can create multiple Layer 3/4 class maps (management or through traffic) for each Layer 3/4 policy map.

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** and **class-map type management** commands.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Use the **class-map type management** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. You can specify a management class map that can match an access list or TCP or UDP ports. A Layer 3/4 class map contains, at most, one **match** command that identifies the traffic included in the class map.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates a Layer 3/4 management class map:

```
hostname(config)# class-map type management radius_acct
hostname(config-cmap)# match port tcp eq 10000
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map for through traffic.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type regex

When using the Modular Policy Framework, group regular expressions for use with matching text by using the **class-map type regex** command in global configuration mode. To delete a regular expression class map, use the **no** form of this command.

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-any	Specifies that the traffic matches the class map if it matches only one of the regular expressions. **match-any** is the only option.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map.

Before you create a regular expression class map, create the regular expressions using the **regex** command. Then, identify the named regular expressions in class-map configuration mode using the **match regex** command.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates two regular expressions, and adds them to a regular expression class map. Traffic matches the class map if it includes the string “example.com” or “example2.com.”

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2
```

Related Commands

Command	Description
class-map type inspect	Creates ain inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
regex	Creates a regular expression.

clear aaa local user fail-attempts

To reset the number of failed user authentication attempts to zero without modifying the user's locked-out status, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command if a user fails to authenticate after a few attempts.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots. The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates, or when the security appliance reboots. Aditionally, the system resets the counter to zero when the configuration has recently been modified.

Locking or unlocking a username results in a system log message. A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for all users:

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user lockout	Resets the number of failed user authentication attempts to zero without modifying the locked-out status of the user.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa local user lockout

To clear the lockout status of the specified users and set their failed-attempts counter to 0, use the **clear aaa local user lockout** command in privileged EXEC mode.

clear aaa local user lockout {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Locking or unlocking a username results in a syslog message.

Examples

The following example shows use of the **clear aaa local user lockout** command to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the locked-out status of the user.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privilged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Clears statistics for the LOCAL user database.
groupname	(Optional) Clears statistics for servers in a group.
host *hostname*	(Optional) Clears statistics for a particular server in the group.
protocol *protocol*	(Optional) Clears statistics for servers of the specificed protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

Remove all AAA-server statistics across all groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines. In the protocol values, **nt** replaces the older **nt-domain**, and **sdi** replaces the older **rsa-ace**.

Examples

The following command shows how to reset the AAA statistics for a specific server in a group:

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following command shows how to reset the AAA statistics for an entire server group:

```
hostname(config)# clear aaa-server statistics svrgrp1
```

The following command shows how to reset the AAA statistics for all server groups:

```
hostname(config)# clear aaa-server statistics
```

The following command shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

Related Commands

Command	Description
aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
clear configure aaa-server	Removes all non-default aaa server groups or clear the specified group
show aaa-server	Displays AAA server statistics.
show running-config aaa-server	Displays the current AAA server configuration values.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configurationmode.

clear access-list [*id*] **counters**

Syntax Description

counters	Clears access list counters.
id	(Optional) Name or number of an access list.

Defaults

All the access list counters are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When you enter the **clear access-list** command, all the access list counters are cleared if you do not specify an *id*.

Examples

The following example shows how to clear a specific access list counter:

```
hostname# clear access-list inbound counters
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the access list configuration that is running on the security appliance.

clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command in privileged EXEC mode.

clear arp [**statistics**]

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears all ARP statistics:

```
hostname# clear arp statistics
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear asp drop

To clear accelerated security path drop statistics, use the **clear asp drop** command in privileged EXEC mode.

clear asp drop [**flow** *type* | **frame** *type*]

Syntax Description

flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped packet statistics.
type	(Optional) Clears the dropped flow or packets statistics for a particular process. See "Usage Guidelines" for a list of types.

Defaults

By default, this command clears all drop statistics.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Process types include the following:

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

Examples

The following example clears all drop statistics:

```
hostname# clear asp drop
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

clear asp table

To clear the hit counters either in asp arp or classify tables, or both, use the **clear asp table** command in privileged EXEC mode.

clear asp table [**arp** | **classify**]

Syntax Description

arp	clears the hits counters in asp arp table only.
classify	clears the hits counters in asp classify tables only

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

There are only two options arp and classify having hits in the **clear asp table** command

Examples

The following example clears all drop statistics:

```
hostname# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

Related Commands

Command	Description
show asp table arp	Shows the contents of the accelerated security path, which might help you troubleshoot a problem.

clear blocks

To reset the packet buffer counters such as the low watermark and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Addtionally, this command clears the history information stored during the last buffer allocation failure.

Examples

The following example clears the blocks:

```
hostname# clear blocks
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics.
show blocks	Shows the system buffer utilization.

clear-button

To customize the Clear button of the WebVPN page login field that is displayed to WebVPN users when they connect to the security appliance, use the **clear-button** command from customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text is “Clear”.

The default style is border:1px solid black;background-color:white;font-weight:bold;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the default background color of the Clear button from black to blue:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# clear-button style background-color:blue
```

Related Commands

Command	Description
login-button	Customizes the login button of the WebVPN page Login field.
login-title	Customizes the title of the WebVPN page Login field.
group-prompt	Customizes the group prompt of the WebVPN page Login field.
password-prompt	Customizes the password prompt of the WebVPN page Login field.
username-prompt	Customizes the username prompt of the WebVPN page Login field.

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command in privileged EXEC configuration mode.

clear capture *capture_name*

Syntax Description

capture_name	Name of the packet capture.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	Support for this command was introduced.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is not supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “example”:

```
hostname(config)# clear capture example
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.

clear compression

To clear compression statistics for all SVC and WebVPN connections, use the **clear compression** command from privileged EXEC mode.

clear compression {**all** | **svc** | **http-comp**}

Syntax Description

all	Clears all compressions statistics.
http-comp	Clears HTTP-COMP statistics.
svc	Clears SVC compression statistics.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example, clears the compression configuration for the user:

```
hostname# clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of data over an SVC connection for a specific group or user.

CHAPTER 6

clear configure through clear configure zonelabs-integrity Commands

clear configure

To clear the running configuration, use the **clear configure** command in global configuration mode.

clear configure {**primary** | **secondary** | **all** | *command*}

Syntax Description

all	Clears the entire running configuration.
command	Clears the configuration for a specified command. For more information, see individual entries in this guide for each **clear configure** *command* command.
primary	Clears commands related to connectivity, including the following commands: • **tftp-server** • **shun** • **route** • **ip address** • **mtu** • **failover** • **monitor-interface** • **boot**
secondary	Clears commands not related to connectivity (that are cleared using the **primary** keyword).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When you enter this command in a security context, you clear only the context configuration. If you enter this command in the system execution space, you clear the system running configuration as well as all context running configurations. Because you cleared all context entries in the system configuration (see the **context** command), the contexts are no longer running, and you cannot change to a context execution space.

Before clearing the configuration, make sure you save any changes to the **boot config** command (which specifies the startup configuration location) to the startup configuration; if you changed the startup configuration location only in the running configuration, then when you restart, the configuration loads from the default location.

Examples

The following example clears the entire running configuration:

```
hostname(config)# clear configure all
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

clear configure aaa

To clear the aaa configuration, use the **clear configure aaa** command in global configuration mode. The **clear configure aaa** command removes the AAA command statements from the configuration.

clear configure aaa

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified for consistency within the CLI.

Usage Guidelines

This command also resets the AAA parameters to their default values, if any.

There is no undo.

Examples

```
hostname(config)# clear configure aaa
```

Related Commands

Command	Description
aaa accounting	Enable, disable, or view the keeping of records about which network services a user has accessed.
aaa authentication	Enable or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication.
aaa authorization	Enable or disable user authorization for a LOCAL or a TACACS+ server designated by the **aaa-server** command, or for ASDM user authentication.
show running-config aaa	Display the AAA configuration.

clear configure aaa-server

To remove all AAA server groups or to clear the specified group, use the **clear configure aaa-server** command in global configuration mode.

clear configure aaa-server [*server-tag*]

clear configure aaa-server [*server-tag*] **host** *server-ip*

Syntax Description

server-ip	The IP address of the AAA server.
server-tag	(Optional) Symbolic name of the server group to be cleared.

Defaults

Remove all AAA server groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can specify a particular AAA server group or, by default, all AAA server groups.

Use the **host** keyword to specify a particular server within a server group.

This command also resets the AAA server parameters to their default values, if any.

Examples

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# sdi-version sdi-5
hostname(config-aaa-server)# exit
```

Given the preceding configuration, the following command shows how to remove a specific server from a group:

```
hostname(config)# clear config aaa-server svrgrp1 host 1.2.3.4
```

The following command shows how to remove a server group:

```
hostname(config)# clear config aaa-server svrgrp1
```

The following command shows how to remove all server groups:

```
hostname(config)# clear config aaa-server
```

Related Commands

Command	Description
aaa-server host	Specifies and manages host-specific AAA server connection data.
aaa-server protocol	Allows you to configure AAA server parameters that are group-specific and common to all hosts.
show running-config aaa	Display the current maximum number of concurrent proxy connections allowed per user, along with other AAA configuration values.

clear configure access-group

To remove access groups from all the interfaces, use the **clear configure access-group** command in global configuration mode.

clear configure access-group

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **configure**.

Examples

The following example shows how to remove all access groups:

```
hostname(config)# clear configure access-group
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
show running-config access-group	Displays the current access group configuration.

clear configure access-list

To clear an access list from the running configuration, use the **clear configure access list** command in global configuration mode.

clear configure access-list [*id*]

Syntax Description

id	(Optional) Name or number of an access list.

Defaults

All the access lists are cleared from the running configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear configure access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** commands referencing the access list are incomplete. To correct the condition, either define other **access-list** commands to complete the **crypto map** commands or remove the **crypto map** commands that pertain to the **access-list** command. Refer to the **crypto map client** command for more information.

Examples

This example shows how to clear the access lists from the running configuration:

```
hostname(config)# clear configure access-list
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear access-list	Clears access list counters.

Command	Description
show access-list	Displays counters for an access list.
show running-config access-list	Displays the access list configuration running on the security appliance.

clear configure alias

To remove all **alias** commands from the configuration, use the **clear configure alias** command in global configuration mode.

clear configure alias

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to remove all **alias** commands from the configuration:

```
hostname(config)# clear configure alias
```

Related Commands

Command	Description
alias	Translates one address into another.
show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.

clear configure arp

To clear static ARP entries added by the **arp** command, use the **clear configure arp** command in global configuration mode.

clear configure arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears static ARP entries from the configuration:

```
hostname(config)# clear configure arp
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear configure arp-inspection

To clear the ARP inspection configuration, use the **clear configure arp-inspection** command in global configuration mode.

clear configure arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the ARP inspection configuration:

```
hostname(config)# clear configure arp-inspection
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear configure asdm

To remove all **asdm** commands from the running configuration, use the **clear configure asdm** command in global configuration mode.

clear configure asdm [**location** | **group** | **image**]

Syntax Description

group	(Optional) Clears only the **asdm group** commands from the running configuration.
image	(Optional) Clears only the **asdm image** command from the running configuration.
location	(Optional) Clears only the **asdm location** commands from the running configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **clear pdm** command to the **clear configure asdm** command.

Usage Guidelines

To view the **asdm** commands in the running configuration, use the **show running-config asdm** command.

Clearing the **asdm image** command from the configuration disables ASDM access. Clearing the **asdm location** and **asdm group** commands from the configuration causes ASDM to regenerate those commands the next time ASDM is accessed, but may disrupt active ASDM sessions.

Note On security appliances running in multiple context mode, the **clear configure asdm image** command is only available in the system execution space, while the **clear configure asdm group** and **clear configure asdm location** commands are only available in the user contexts.

Examples

The following example clears the **asdm group** commands from the running configuration:

```
hostname(config)# clear configure asdm group
```

```
hostname(config)#
```

Related Commands

Command	Description
asdm group	Used by ASDM to associate object group names with interfaces.
asdm image	Specifies the ASDM image file.
asdm location	Used by ASDM to record IP address to interface associations.
show running-config asdm	Displays the **asdm** commands in the running configuration.

clear configure auth-prompt

To remove the previously specified authentication prompt challenge text and revert to the default value, if any, use the **clear configure auth-prompt** command in global configuration mode.

clear configure auth-prompt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to conform with CLI standards.

Usage Guidelines

After you clear the authentication prompt, the prompt users see when they log in depends on the protocol they use:

- Users who log in using HTTP see `HTTP Authentication`.
- Users who log in using FTP see `FTP Authentication`.
- Users who log in using Telnet see no prompt.

Examples

This example shows how to clear the auth-prompt:

```
hostname(config)# clear configure auth-prompt
```

Related Commands

auth-prompt	Sets the user authorization prompts.
show running-config auth-prompt	Displays the user authorization prompts.

clear configure banner

To remove all the banners, use the **clear configure banner** command in global configuration mode.

clear configure banner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to clear banners:

```
hostname(config)# clear configure banner
```

Related Commands

Command	Description
banner	Configures the session, login, or message-of-the-day banner.
show running-config banner	Displays all banners.

clear configure ca certificate map

To remove all certificate map entries or to remove a specified certificate map entry, use the **clear configure ca configurate map** command in global configuration mode.

clear configure ca certificate map [*sequence-number*]

Syntax Description

sequence-number	(Optional) Specifies a number for the certificate map rule you are removing. The range is 1 through 65535.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example removes all certificate map entries.

```
hostname(config)# clear configure ca certificate map
hostname(config)#
```

Related Commands+

Command	Description
crypto ca certificate map	Enters CA certificate map mode.

clear configure class

To clear the resource class configuration, use the **clear configure class** command in global configuration mode.

clear configure class

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears the class configuration:

```
hostname(config)# clear configure class
```

Related Commands

Command	Description
class	Configures a resource class.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.
show class	Shows the contexts assigned to a class.

clear configure class-map

To remove all class maps, use the **clear configure class-map** command in global configuration mode.

clear configure class-map [**type** {**management** | **regex** | **inspect** [*protocol*]}

Syntax Description

inspect	(Optional) Clears inspection class maps.
management	(Optional) Clears management class maps.
protocol	(Optional) Specifies the type of application map you want to clear. Available types include: • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	(Optional) Clears regular expression class maps.
type	(Optional) Specifies the type of class map you want to clear. To clear Layer 3/4 class maps, to not specify the type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To clear the class map for a specific class map name, use the **no** form of the **class-map** command.

Examples

The following example shows how to clear all configured class maps:

```
hostname(config)# clear configure class-map
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
show running-config class-map	Displays the information about the class map configuration.

clear configure client-update

To remove from the configuration the ability to force a client update, use the **clear configure client-update** command in global configuration mode or tunnel-group ipsec-attributes configuration mode.

clear configure client-update

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added tunnel-group ipsec-attributes configuration mode.

Examples

The following example entered in global configuration mode, removes the client-update capability from the configuration:

```
hostname(config)# clear configure client-update
hostname(config)#
```

The following example entered in tunnel-group ipsec-attributes configuration mode, removes the client-update capability from the configuration of the tunnel group named test:

```
hostname(config)# tunnel-group test ipsec-attributes
hostname(config-tunnel-ipsec)# clear configure client-update
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
client-update	Configures client-update.
show running-config client-update	Shows the current client-update configuration.

clear configure clock

To clear the clock configuration, use the **clear configure clock** command in global configuration mode.

clear configure clock

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from **clear clock**.

Usage Guidelines

This command clears all **clock** configuration commands. The **clock set** command is not a configuration command, so this command does not reset the clock. To reset the clock, you need to set a new time for the **clock set** command.

Examples

The following example clears all clock commands:

```
hostname# clear configure clock
```

Related Commands

Command	Description
clock set	Manually sets the time.
clock summer-time	Sets the date range to show daylight savings time.
clock timezone	Sets the time zone.

clear configure command-alias

To remove all non-default command aliases, use the **clear configure command-alias** command in global configuration mode.

clear configure command-alias

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows how to remove all non-default command aliases:

```
hostname(config)# clear configure command-alias
```

Related Commands

Command	Description
command-alias	Creates a command alias.
show running-config command-alias	Displays all non-default command aliases.

clear configure compression

To reset the global compression configuration to the default (all compression techniques enabled), use the **clear configure compression** command from global configuration mode:

clear configure compression

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

In the following example, the compression configuration is cleared:

```
hostname(config)# clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and Port Forwarding connections.
svc compression	Enables compression of http data over an SVC connection for a specific group or user.

clear configure console

To reset the console connection settings to defaults, use the **clear configure console** command in global configuration mode.

clear configure console

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to reset the console connection settings to defaults:

```
hostname(config)# clear configure console
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the security appliance.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

clear configure context

To clear all context configurations in the system configuration, use the **clear configure context** command in global configuration mode.

clear configure context [**noconfirm**]

Syntax Description

noconfirm	(Optional) Removes all contexts without prompting you for confirmation. This option is useful for automated scripts.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command lets you remove all contexts, including the admin context. The admin context cannot be removed using the **no context** command, but can be removed using the **clear configure context** command.

Examples

The following example removes all contexts from the system configuration, and does not confirm the deletion:

```
hostname(config)# clear configure context noconfirm
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
context	Creates a security context in the system configuration and enters context configuration mode.

Command	Description
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

clear configure crypto

To remove the entire crypto configuration, including IPSec, crypto maps, dynamic crypto maps, CA trstpoints, all certificates, certificate map configurations, and ISAKMP, use the **clear configure crypto** command in global configuration. To remove specific configurations, use this command with keywords as shown in the syntax. Take caution when using this command.

clear configure crypto [**ca** | **dynamic-map** | **ipsec** | **iskmp** | **map**]

Syntax Description

ca	Removes certification authority policy.
dynamic-map	Removes dynamic crypto map configuration.
ipsec	Removes IPSec configuration.
isakmp	Removes ISAKMP configuration.
map	Removes crypto map configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example issued in global configuration mode, removes all of the crypto configuration from the security appliance:

```
hostname(config)# clear configure crypto
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all or specified crypto dynamic maps from the configuration.
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
show running-config crypto	Displays the entire crypto configuration, including IPSec, crypto maps, dynamic crypto maps, and ISAKMP.

clear configure crypto ca trustpoint

To remove all trustpoints from the configuration, use the **clear configure crypto ca trustpoint** command in global configuration.

clear configure crypto ca trustpoint

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, removes all trustpoints from the configuration:

```
hostname(config)# clear configure crypto ca trustpoint
hostname(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint subconfiguration level for the indicated trustpoint.

clear configure crypto dynamic-map

To remove all or specified crypto dynamic maps from the configuration, use the **clear configure crypto dynamic-map** command in global configuration.

clear configure crypto dynamic-map *dynamic-map-name dynamic-seq-num*

Syntax Description

dynamic-map-name	Specifies the name of a specific crypto dynamic map.
dynamic-seq-num	Specifies the sequence number of the crypto dynamic map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, removes the crypto dynamic map mymaps with sequence number 3 from the configuration:

```
hostname(config)# clear configure crypto dynamic-map mymaps 3
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears the configuration of all or specified crypto maps.
show running-config crypto dynamic-map	Displays all the active configuration for all dynamic crypto maps.
show running-config crypto map	Displays all the active configuration for all crypto maps.

clear configure crypto isakmp

To remove all of the ISAKMP configuration, use the **clear configure crypto isakmp** command in global configuration mode.

clear configure crypto isakmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **clear configure isakmp** command was introduced.
7.2(1)	This command was deprecated. The **clear configure crypto isakmp** command replaces it.

Examples

The following command, issued in global configuration mode, removes all of the ISAKMP configuration from the security appliance:

```
hostname(config)# clear configure crypto isakmp
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show crypto isakmp stats	Displays runtime statistics.
show crypto isakmp sa	Displays IKE runtime SA database with additional information.
show running-config crypto isakmp	Displays all the active configuration.

clear configure crypto isakmp policy

To remove all of the ISAKMP policy configuration, use the **clear configure isakmp policy** command in global configuration mode.

clear configure crypto isakmp policy *priority*

Syntax Description

priority	Specifies the priority of the ISAKMP priority to be cleared.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **clear configure isakmp policy** command was introduced.
7.2(1)	The **clear configure crypto isakmp policy** command replaces the **clear configure isakmp policy** command.

Examples

The following example removes the ISAKMP policy with priority 3 from the configuration:

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

Related Commands

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active configuration.

clear configure crypto map

To remove all or specified crypto maps from the configuration, use the **clear configure crypto map** command in global configuration.

clear configure crypto map *map-name seq-num*

Syntax Description

map-name	Specifies the name of a specific crypto map.
seq-num	Specifies the sequence number of the crypto map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, removes the crypto map mymaps with sequence number 3 from the configuration:

```
hostname(config)# clear configure crypto map mymaps 3
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears the configuration of all or specified crypto dynamic maps.
crypto map interface	Applies a crypto map to an interface.
show running-config crypto map	Displays the active configuration for all crypto maps.
show running-config crypto dynamic-map	Displays the active configuration for all dynamic crypto maps.

clear configure ctl-file

To clear configured CTL file instances, use the **clear configure ctl-file** command in global configuration mode.

clear configure ctl [*ctl_name***]**

Syntax Description

ctl_name	(Optional) Specifies the name of the CTL instance.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **clear configure ctl-file** command to clear configured CTL file instances:

```
hostname# clear configure ctl asa_phone_proxy asa_ctl
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

clear configure ctl-provider

To remove all configured Certificate Trust List provider instances, use the **clear configure ctl-provider** command in global configuration mode.

clear configure ctl-provider

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows the syntax of the **clear configure ctl-provider** command:

```
hostname# clear configure ctl-provider
```

Related Commands

Command	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.

clear configure ddns

To clear all DDNS commands, use the **clear configure ddns** command in global configuration mode.

clear configure ddns

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears all DDNS commands:

```
hostname(config)# clear configure ddns
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a security appliance interface with a DDNS update method or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show ddns update interface	Displays the interfaces associated with each configured DDNS method.
show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

clear configure dhcpd

To clear all of the DHCP server commands, binding, and statistics, use the **clear configure dhcpd** command in global configuration mode.

clear configure dhcpd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear dhcpd** to **clear configure dhcpd**.

Usage Guidelines

The **clear configure dhcpd** command clears all of the **dhcpd** commands, bindings, and statistical information. To clear only the statistic counters or binding information, use the **clear dhcpd** command.

Examples

The following example shows how to clear all **dhcpd** commands:

```
hostname(config)# clear configure dhcpd
```

Related Commands

Command	Description
clear dhcpd	Clears the DHCP server bindings and statistic counters.
show running-config dhcpd	Displays the current DHCP server configuration.

clear configure dhcprelay

To clear all of the DHCP relay configuration, use the **clear configure dhcprelay** command in global configuration mode.

clear configure dhcprelay

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear dhcprelay** to **clear configure dhcprelay**.

Usage Guidelines

The c**lear configure dhcprelay** command clears the DHCP relay statistics and configuration. To clear only the DHCP statistic counters, use the **clear dhcprelay statistics** command.

Examples

The following example shows how to clear the DHCP relay configuration:

```
hostname(config)# clear configure dhcprelay
```

Related Commands

Command	Description
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear configure dns

To clear all DNS commands, use the **clear configure dns** command in global configuration mode.

clear configure dns

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears all DNS commands:

```
hostname(config)# clear configure dns
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

clear configure dynamic-access-policy-config

To clear the DAP configuration, use the **clear configure dynamic-access-policy-config** command in dynamic-access-policy-record configuration mode.

clear config dynamic-access-policy-config *name*

Syntax Description

name	A string that specifies the name of the DAP configuration file.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dynamic-access-policy-record configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows how to set a priority of 15 for the DAP record called Finance.

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# priority 15
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

clear config dynamic-access-policy-record

To clear a DAP record, use the **clear config dynamic-access-policy-record** command in global configuration mode with the name of the record. To clear all DAP records, use the **no** form of this command.

clear config dynamic-access-policy-record *name*

Syntax Description

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows how to clear a DAP record named Finance.

```
hostname(config)# clear configure dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record [*name***]**	Creates a named DAP record.
dynamic-access-policy-config url	Configures the DAP Selection Configuration file.
show running-config dynamic-access-policy-record [*name***]**	Displays the running configuration for all DAP records, or for the named DAP record.

clear configure established

To remove all established commands, use the **clear configure established** command in global configuration mode.

clear configure established

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The keyword **configure** was added.

Usage Guidelines

To remove an established connection created by the **established** command, enter the **clear xlate** command.

Examples

This example shows how to remove established commands:

```
hostname(config)# clear configure established
```

Related Commands

Command	Description
established	Permits return connections on ports that are based on an established connection.
show running-config established	Displays the allowed inbound connections that are based on established connections.
clear xlate	Clears the current translation and connection slot information.

clear configure failover

To remove **failover** commands from the configuration and restore the defaults, use the **clear configure failover** command in global configuration mode.

clear configure failover

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	Command was changed from **clear failover** to **clear configure failover**.

Usage Guidelines

This command clears all **failover** commands from the running configuration and restores the defaults. If you use the **all** keyword with the **show running-config failover** command, you will see the default failover configuration.

The **clear configure failover** command is not available in a security context in multiple configuration mode; you must enter the command in the system execution space.

Examples

The following example clears all failover commands from the configuration:

```
hostname(config)# clear configure failover
hostname(config)# show running-configuration failover
no failover
```

Related Commands

Command	Description
show running-config failover	Displays the **failover** commands in the running configuration.

clear configure filter

To clear URL, FTP, and HTTPS filtering configuration, use the **clear configure filter** command in global configuration mode.

clear configure filter

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure filter** command clears the URL, FTP, and HTTPS filtering configuration.

Examples

The following example clears the URL, FTP, and HTTPS filtering configuration:

```
hostname(config)# clear configure filter
```

Related Commands

Commands	Description
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays the filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear configure fips

To clear the system or module FIPS configuration information stored in NVRAM, use the **clear configure fips** command in global configuration mode.

clear configure fips

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Examples

```
hostname(config)# clear configure fips
```

Related Commands

Command	Description
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

clear configure firewall

To set the firewall mode to the default routed mode, use the **clear configure firewall** command in global configuration mode.

clear configure firewall

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the firewall mode to the default:

```
hostname(config)# clear configure firewall
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear configure fixup

To clear the fixup configuration, use the **clear configure fixup** command in global configuration mode.

clear configure fixup

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear configure fixup** command removes the fixup configuration.

Examples

The following example clears the fixup configuration:

```
hostname# clear configure fixup
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.

clear configure fragment

To reset all the IP fragment reassembly configurations to defaults, use the **clear configure fragment** command in global configuration mode.

clear configure fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The **configure** keyword and optional *interface* argument were added. The command was also separated into two commands, **clear fragment** and **clear configure fragment**, to separate clearing of the configuration data from the operational data.

Usage Guidelines

The **clear configure fragment** command resets all the IP fragment reassembly configurations to defaults. In addition, the the **chain**, **size**, and **timeout** keywords are reset to their default values, which are as follows:

- **chain** is 24 packets
- **size** is 200
- **timeout** is 5 seconds

Examples

This example shows how to reset all the IP fragment reassembly configurations to defaults:

```
hostname(config)# clear configure fragment
```

Related Commands

Command	Description
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.

Command	Description
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear configure ftp

To clear the FTP configuration, use the **clear configure ftp** command in global configuration mode.

clear configure ftp

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure ftp** command clears the FTP configuration.

Examples

The following example clears the FTP configuration:

```
hostname# clear configure ftp
```

Related Commands

Commands	Description
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays the filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear configure global

To remove the **global** commands from the configuration, use the **clear configure global** command in global configuration mode.

clear configure global

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **configure**.

Examples

The following example shows how to remove the **global** commands from the configuration:

```
hostname(config)# clear configure global
```

Related Commands

Command	Description
global	Creates entries from a pool of global addresses.
show running-config global	Displays the **global** commands in the configuration.

clear configure group-delimiter

To remove from the configuration the group delimiter the delimiter used when parsing group names from the user names that are received when tunnels are being negotiated, use the **clear configure group-delimiter** command in global configuration mode. This disables group-name parsing.

clear config group-delimiter

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The delimiter is used to parse tunnel group names from usernames when tunnels are negotiated. If no delimiter is specified, group-name parsing is disabled.

Examples

The following example entered in global configuration mode, removes the group delimiter from the configuration:

```
hostname(config)# clear config group-delimiter
hostname(config)#
```

Related Commands

Command	Description
group-delimiter	Enables group-name parsing and specifies the group delimiter for an IPSec remote access tunnel group.
show running-config group-delimiter	Shows the current configured group delimiter.

clear configure group-policy

To remove the configuration for a particular group policy, use the **clear configure group-policy** command in global configuration mode, and append the name of the group policy. To remove all group-policy commands from the configuration except the default group policy, use this command without arguments.

clear configure group-policy [*name*]

Syntax Description

name	(Optional) Specifies the name of the group policy.

Defaults

Remove all group-policy commands from the configuration, except the default group policy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to clear the configuration for the group policy named FirstGroup.

```
hostname(config)# clear configure group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Creates, edits, or removes a group policy.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.

clear configure hostname

To reset the hostname to the default, use the **clear configure hostname** command in global configuration mode.

clear configure hostname

Syntax Description

This command has no arguments or keywords.

Defaults

The default value depends on your platform.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the hostname:

```
hostname(config)# clear configure hostname
```

Related Commands

Command	Description
banner	Sets a login, message of the day, or enable banner.
domain-name	Sets the default domain name.
hostname	Sets the hostname for the security appliance.

clear configure http

To disable the HTTP server and to remove configured hosts that can access the HTTP server, use the **clear configure http** command in global configuration mode.

clear configure http

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to clear the HTTP configuration.

```
hostname(config)# clear configure http
```

Related Commands

Command	Description
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

clear configure icmp

To clear the configured access rules for ICMP traffic, use the **clear configure icmp** command in global configuration mode.

clear configure icmp

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure icmp** command clears the configured access rules for ICMP traffic.

Examples

The following example clears the clear configured access rules for ICMP traffic:

```
hostname# clear configure icmp
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

clear configure imap4s

To remove all IMAP4S commands from the configuration, reverting to default values, use the **clear configure imap4s** command in global configuration mode.

clear configure imap4s

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the IMAP4S configuration:

```
hostname(config)# clear configure imap4s
hostname(config)#
```

Related Commands

Command	Description
show running-configuration imap4s	Displays the running configuration for IMAP4S.
imap4s	Creates or edits an IMAP4S e-mail proxy configuration.

clear configure interface

To clear the interface configuration, use the **clear configure interface** command in global configuration mode.

clear configure interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance clears all interface configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from **clear interface**. This command was also modified to include the new interface numbering scheme.

Usage Guidelines

When you clear the interface configuration for main physical interfaces, the security appliance uses the default settings.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears the GigabitEthernet0/1 configuration:

```
hostname(config)# clear configure interface gigabitethernet0/1
```

The following example clears the inside interface configuration:

```
hostname(config)# clear configure interface inside
```

The following example clears the int1 interface configuration in a context. “int1” is a mapped name.

```
hostname/contexta(config)# clear configure interface int1
```

The following example clears all interface configuration.

```
hostname(config)# clear configure interface
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

clear configure ip

To clear all IP addresses set by the **ip address** command, use the **clear configure ip** command in global configuration mode.

clear configure ip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In transparent firewall mode, this command clears the management IP address and the Management 0/0 IP address, if configured.

If you want to stop all current connections that use the old IP addresses, enter the **clear xlate** command. Otherwise, the connections time out as usual.

Examples

The following example clears all IP addresses:

```
hostname(config)# clear configure ip
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface.
show running-config interface	Displays the interface configuration.

clear configure ip audit

To clear the entire audit policy configuration, use the **clear configure ip audit** command in global configuration mode.

clear configure ip audit [**configuration**]

Syntax Description

configuration	(Optional) Yuo can enter this keyword, but the effect is the same without it.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear ip audit**.

Examples

The following example clears all **ip audit** commands:

```
hostname# clear configure ip audit
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

clear configure ip local pool

To remove IP address pools, use the **clear configure ip local pool** command in global configuration mode.

clear ip local pool [*poolname*]

Syntax Description

poolname	(Optional) Specifies the name of the IP address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example removes all IP address pools from the running configuration:

```
hostname(config)# clear config ip local pool
hostname(config)#
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools.
ip local pool	Configures an IP address pool.

clear configure ip verify reverse-path

To clear the **ip verify reverse-path** configuration, use the **clear configure ip verify reverse-path** command in global configuration mode.

clear configure ip verify reverse-path

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear ip verify reverse-path**.

Examples

The following example clears the **ip verify reverse-path** configuration for all interfaces:

```
hostname(config)# clear configure ip verify reverse-path
```

Related Commands

Command	Description
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

clear configure ipv6

To clear the global IPv6 commands from the running configuration, use the **clear configure ipv6** command in global configuration mode.

clear configure ipv6 [**route** | **access-list**]

Syntax Description

access-list	(Optional) Clears the IPv6 access list commands from the running configuration.
route	(Optional) Clears the commands that statically define routes in the IPv6 routing table from the running configuration.

Defaults

Without keywords, this command clears all IPv6 commands from the running configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command only clears the global IPv6 commands from the running configuration; it does not clear the IPv6 commands entered in interface configuration mode.

Examples

The following example shows how to clear statically defined IPv6 routes from the IPv6 routing table:

```
hostname(config)# clear configure ipv6 route
hostname(config)#
```

Related Commands

Command	Description
ipv6 route	Defines a static route in the IPv6 routing table.
show ipv6 route	Displays the contents of the IPv6 routing table.
show running-config ipv6	Displays the IPv6 commands in the running configuration.

clear configure isakmp

To remove all of the ISAKMP configuration, use the **clear configure isakmp** command in global configuration mode.

clear configure isakmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **clear configure isakmp** command was introduced.
7.2(1)	This command was deprecated. The **clear configure crypto isakmp** command replaces it.

Examples

The following example issued in global configuration mode, removes all of the ISAKMP configuration from the security appliance:

```
hostname(config)# clear configure isakmp
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp policy	Clears all ISAKMP policy configuration.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active configuration.

clear configure isakmp policy

To remove all of the ISAKMP policy configuration, use the **clear configure isakmp policy** command in global configuration mode.

clear configure isakmp policy *priority*

Syntax Description

priority	Specifies the priority of the ISAKMP priority to be cleared.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **clear configure isakmp policy** command was introduced.
7.2(1)	This command was deprecated. The **clear configure crypto isakmp policy** command replaces it.

Examples

The following example removes the ISAKMP policy with priority 3 from the configuration:

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

Related Commands

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active configuration.

clear configure ldap attribute-map

To remove all the LDAP attribute maps from the running configuration of the security appliance, use the **clear configure ldap attribute-map** command in global configuration mode.

clear configure ldap attribute-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to remove the LDAP attribute maps from the running configuration of the security appliance.

Examples

The following example, entered in global configuration mode, removes all LDAP attributes map from the running configuration and then confirms the removal by using the **show running-config ldap attribute-map** command:

```
hostname(config)# clear configuration ldap attribute-map
hostname(config)# show running-config ldap attribute-map
hostname(config)#
```

Related Commands

Command	Description
ldap attribute-map (global config mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.

Command	Description
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.

clear configure logging

To clear logging configuration, use the **clear configure logging** command in global configuration mode.

clear configure logging [**disabled** | **level**]

Syntax Description

disabled	(Optional) Indicates that all disabled system log messages should be re-enabled. When you use this option, no other logging configuration is cleared.
level	(Optional) Indicates that the severity level assignments for system log messages should be reset to their default values. When you use this option, no other logging configuration is cleared.

Defaults

With no keywords specified, this command returns all configuration settings to their default values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can use the **show running-config logging** command to view all logging configuration settings. If you use the **clear configure logging** command without either the disabled or level keyword, all logging configuration settings are cleared and returned to their default values.

Examples

The following example shows how to clear logging configuration settings. The output of the **show logging** command indicates that all logging features are disabled.

```
hostname(config)# clear configure logging
hostname(config)# show logging
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
```

```
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

clear configure logging rate-limit

To reset the logging rate limit, use the **clear configure logging rate-limit** command in global configuration mode.

clear configure logging rate-limit

Syntax DescriptionT

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Examples

The following example shows how to reset the logging rate limit:

```
hostname(config)# clear configure logging rate-limit
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

Command	Description
logging rate limit	Limits the rate at which system log messages are generated.
show running config logging rate-limit	Shows the current logging rate limit setting.

clear configure mac-address-table

To clear the **mac-address-table static** and **mac-address-table aging-time** configuration, use the **clear configure mac-address-table** command in global configuration mode.

clear configure mac-address-table

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the **mac-address-table static** and **mac-address-table aging-time** configuration:

```
hostname# clear configure mac-address-table
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning for an interface.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

clear configure mac-learn

To clear the **mac-learn** configuration, use the **clear configure mac-learn** command in global configuration mode.

clear configure mac-learn

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the **mac-learn** configuration:

```
hostname# clear configure mac-learn
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning for an interface.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

clear configure mac-list

To remove the indicated list of MAC addresses, previously specified the **mac-list** command, use the **clear configure mac-list** command in global configuration mode:

clear configure mac-list *id*

Syntax Description

id	A MAC address list name.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to conform with CLI standards.

Usage Guidelines

To remove a list of MAC addresses, use the **clear mac-list** command.

Examples

The following example shows how to clear a MAC address list:

```
hostname(config)# clear configure mac-list firstmaclist
```

Related Commands

Command	Description
mac-list	Adds a list of MAC addresses using a first-match search.
show running-config mac-list	Displays the MAC addresses in the MAC address list indicated by the *id* value.

clear configure management-access

To remove the configuration of an internal interface for management access of the security appliance, use the **clear configure management-access** command in global configuration mode.

clear configure management-access

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The keyword **configure** was added.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.) The **clear configure management-access** command removes the configuration of the internal management interface specified with the **management-access** command.

Examples

The following example removes the configuration of an internal interface for management access of the security appliance:

```
hostname(config)# clear configure management-access
```

Related Commands

Command	Description
management-access	Configures an internal interface for management access.
show running-config management-access	Displays the name of the internal interface configured for management access.

clear configure monitor-interface

To remove all **monitor-interface** commands from the running configuration and restore the default interface health monitoring, use the **clear configure monitor-interface** command in global configuration mode.

clear configure monitor-interface

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

By default, physical interfaces are monitored for failover. Using the **clear monitor-interface** command clears the **no monitor-interface** commands from the running configuration and restores default interface health monitoring. To view the **monitor-interface** commands in the running configuration, use the **show running-config all monitor-interface** command.

Examples

The following example clears the **monitor-interface** commands from the running configuration:

```
hostname(config)# clear configure monitor-interface
hostname(config)#
```

Related Commands

Command	Description
monitor-interface	Enables health monitoring of a designated interface for failover purposes.
show running-config monitor-interface	Displays the **monitor-interface** commands in the running configuration.

clear configure mroute

To remove the **mroute** commands from the running configuration, use the **clear configure mroute** command in global configuration mode.

clear configure mroute

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the **mroute** commands from the configuration:

```
hostname(config)# clear configure mroute
hostname(config)#
```

Related Commands

Command	Description
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays the **mroute** commands in the running configuration.

clear configure mtu

To clear the configured maximum transmission unit values on all interfaces, use the **clear configure mtu** command in global configuration mode.

clear configure mtu

Syntax Description

This command has no arguments or keywords.

Defaults

Using the clear configure mtu command sets the maximum transmission unit to the default of 1500 for all Ethernet interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the current maximum transmission unit values on all interfaces:

```
hostname(config)# clear configure mtu
```

Related Commands

Command	Description
mtu	Specifies the maximum transmission unit for an interface.
show running-config mtu	Displays the current maximum transmission unit block size.

clear configure multicast-routing

To remove the **multicast-routing** command from the running configuration, use the **clear configure multicast-routing** command in global configuration mode.

clear configure multicast-routing

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The clear configure multicast-routing command removes the multicast-routing from the running configuration. The no multicast-routing command also removes the multicast-routing command from the running configuration.

Examples

The following example shows how to remove the **multicast-routing** command from the running configuration:

```
hostname(config)# clear configure multicast-routing
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

clear configure nac-policy

To remove all NAC policies from the running configuration, except for those that are assigned to group policies, use the **clear configure nac-policy** command in global configuration mode.

clear configure nac-policy

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use this command only if you want to remove all NAC policies. Use the **no** version of the nac-policy command to remove a single NAC policy from the configuration.

Examples

The following command shows how to remove all NAC policies:

```
hostname(config)# clear config nac-policy
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
show nac-policy	Displays NAC policy usage statistics on the security appliance.
show running-config nac-policy	Displays the configuration of each NAC policy on the security appliance.
show vpn-session_summary.db	Displays the number IPSec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

clear configure name

To clear the list of names from the configuration, use the **clear configure name** command in global configuration mode.

clear configure name

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **configure** was added.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows how to clear the name list:

```
hostname(config)# clear configure name
```

Related Commands

Command	Description
name	Associates a name with an IP address.
show running-config name	Displays the list of names associated with IP addresses.

clear configure nat

To remove the NAT configuration, use the **clear configure nat** command in global configuration mode.

clear configure nat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **configure**.

Usage Guidelines

The following applies to transparent firewall mode:

Note In transparent firewall mode, only NAT id 0 is valid.

Examples

The following example shows how to remove the NAT configuration:

```
hostname(config)# clear configure nat
```

Related Commands

Command	Description
nat	Associates a network with a pool of global IP addresses.
show running-config nat	Displays a pool of global IP addresses that are associated with the network.

clear configure nat-control

To disable the NAT configuration requirement, use the **clear configure nat-control** command in global configuration mode.

clear configure nat-control

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example disables the NAT configuration requirement:

```
hostname(config)# clear configure nat-control
```

Related Commands

Command	Description
nat	Defines an address on one interface that is translated to a global address on another interface.
nat-control	Enforces NAT control. Disabling NAT control allows inside hosts to communicate with outside networks without configuring a NAT rule.
show running-config nat-control	Displays the NAT configuration requirement.

clear configure ntp

To clear the NTP configuration, use the **clear configure ntp** command in global configuration mode.

clear configure ntp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from **clear ntp**.

Examples

The following example clears all **ntp** commands:

```
hostname# clear configure ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets the NTP authentication key.
ntp server	Identifies an NTP server to set the time on the security appliance.
ntp trusted-key	Specifies the NTP trusted key.
show running-config ntp	Shows the NTP configuration.

clear configure object-group

To remove all the **object group** commands from the configuration, use the **clear configure object-group** command in global configuration mode.

clear configure object-group [**protocol** | **service** | **icmp-type** | **network**]

Syntax Description

icmp-type	(Optional) Clears all ICMP groups.
network	(Optional) Clears all network groups.
protocol	(Optional) Clears all protocol groups.
service	(Optional) Clears all service groups.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to remove all the **object-group** commands from the configuration:

```
hostname(config)# clear configure object-group
```

Related Commands

Command	Description
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

clear configure passwd

To clear the login password configuration and restore the default setting of "cisco," use the **clear configure passwd** command in global configuration mode.

clear configure {**passwd** | **password**}

Syntax Description

passwd | **password**	You can enter either command; they are aliased to each other.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from **clear passwd**.

Examples

The following example clears the login password and restores it to the default of "cisco":

```
hostname(config)# clear configure passwd
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
passwd	Sets the login password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

clear configure phone-proxy

To clear Phone Proxy configuration, use the **clear configure phone-proxy** command in global configuration mode.

clear configure phone-proxy [*phone_proxy_name*]

Syntax Description

phone_proxy_name	Specifies the name of the Phone Proxy instance.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **clear configure phone-proxy** command to clear the Phone Proxy configuration:

```
hostname# clear configure phone-proxy asa_phone_proxy
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

clear configure pim

To clear all of the global **pim** commands from the running configuration, use the **clear configure pim** command in global configuration mode.

clear configure pim

Syntax Description

There are no keywords or arguments for this command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure pim** command clears all of the **pim** commands from the running configuration. To clear PIM traffic counters and topology information, use the **clear pim counters** and the **clear pim topology** commands.

The **clear configure pim** command only clears the **pim** commands entered in global configuration mode; it does not clear the interface-specific **pim** commands.

Examples

The following example shows how to clear all **pim** commands from the running configuration:

```
hostname(config)# clear configure pim
```

Related Commands

Command	Description
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears the PIM traffic counters.
show running-config pim	Displays the **pim** commands in the running configuration.

clear configure policy-map

To remove the all **policy-map** commands, use the **clear configure policy-map** command in global configuration mode.

clear configure policy-map [**type inspect** [*protocol*]}

Syntax Description

type inspect	(Optional) Clears inspection policy maps.
protocol	(Optional) Specifies the type of inspection policy map you want to clear. Available types include: • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To clear the policy map for a specific policy map name, use the **no** form of the **policy-map** command.

Examples

The following example shows the **clear configure policy-map** command:

```
hostname(config)# clear configure policy-map
```

Related Commands

Command	Description
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays the entire policy configuration.

clear configure pop3s

To remove all POP3S commands from the configuration, reverting to default values, use the **clear configure pop3s** command in global configuration mode.

clear configure pop3s

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the POP3S configuration:

```
hostname(config)# clear configure pop3s
hostname(config)#
```

Related Commands

Command	Description
show running-configuration pop3s	Displays the running configuration for POP3S.
pop3s	Creates or edits a POP3S e-mail proxy configuration.

clear configure prefix-list

To remove the **prefix-list** commands from the running configuration, use the **clear configure prefix-list** command in global configuration mode.

clear configure prefix-list [*prefix_list_name*]

Syntax Description

prefix_list_name	(Optional) The name of a prefix list. When a prefix list name is specified, only the commands for that prefix list are removed from the configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear prefix-list** to **clear configure prefix-list**.

Usage Guidelines

The **clear configure prefix-list** command removes the **prefix-list** commands and the **prefix-list description** commands from the running configuration. If a prefix list name is specified, then the **prefix-list** command and **prefix-list description** command, if present, for that prefix list only are removed from the running configuration.

This command does not remove the **no prefix-list sequence** command from the running configuration.

Examples

The following example removes all **prefix-list** commands from the running configuration for a prefix list named MyPrefixList:

```
hostname# clear configure prefix-list MyPrefixList
```

Related Commands

Command	Description
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

clear configure priority-queue

To remove the priority queue specification from the configuration, use the **clear configure priority-queue** command in global configuration mode.

clear configure priority queue *interface-name*

Syntax Description

interface-name	Specifies the name of the interface for which you want to show the priority queue details

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the **clear configure priority-queue** command to remove the priority-queue configuration on the interface named test:

```
hostname(config)# clear configure priority-queue test
```

Related Commands

Command	Description
priority-queue	Configures priority queueing on an interface.
show running-config priority-queue	Displays the current priority-queue configuration for the named interface.

clear configure privilege

To remove the configured privilege levels for commands, use the **clear configure privilege** command in global configuration mode.

clear configure privilege

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

There is no undo.

Examples

This example shows how to reset the configured privilege levels for the commands:

```
hostname(config)# clear configure privilege
```

Related Commands

Command	Description
privilege	Configures the command privilege levels.
show curpriv	Displays current privilege level
show running-config privilege	Displays privilege levels for commands.

clear configure regex

To remove all regular expressions, use the **clear configure regex** command in global configuration mode.

clear configure regex

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To clear the regular expression for a specific regular expression name, use the **no** form of the **regex** command.

Examples

The following example shows how to clear all configured regular expressions:

```
hostname(config)# clear configure regex
```

Related Commands

Command	Description
class-map type regex	Creates a regular expression class map.
regex	Creates a regular expression.
show running-config regex	Shows all regular expressions.
test regex	Tests a regular expression.

clear configure route

To remove the **route** commands from the configuration that do not contain the **connect** keyword, use the **clear configure route** command in global configuration mode.

clear configure route [*interface_name ip_address* [*netmask gateway_ip*]]

Syntax Description

gateway_ip	(Optional) Specifies the IP address of the gateway router (the next hop address for this route).
interface_name	(Optional) Internal or external network interface name.
ip_address	(Optional) Internal or external network IP address.
netmask	(Optional) Specifies a network mask to apply to the *ip_address*.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **configure**.

Usage Guidelines

Use **0.0.0.0** to specify a default route. You can abbreviate the 0.0.0.0 IP address as **0** and the 0.0.0.0 *netmask* as **0.**

Examples

The following example shows how to remove the **route** commands from the configuration that do not contain the **connect** keyword:

```
hostname(config)# clear configure route
```

Related Commands

Command	Description
route	Specifies a static or default route for the an interface.
show route	Displays route information.
show running-config route	Displays configured routes.

clear configure route-map

To remove all of the route maps, use the **clear configure route-map** command in global configuration mode.

clear configure route-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **clear configure route-map** command in global configuration mode to remove all the **route-map** commands in the configuration. The **route-map** command is used to configure conditions of redistributing the routes from one routing protocol into another routing protocol.

To remove the individual **route-map** commands, use the **no route-map** command.

Examples

The following example shows how to remove the conditions of redistributing routes from one routing protocol into another routing protocol:

```
hostname(config)# clear configure route-map
```

Related Commands

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
show running-config route-map	Displays information about the route map configuration.

clear configure router

To clear the router configuration commands from the running configuration, use the **clear configure router** command in global configuration mode.

clear configure router [**ospf** [*id*] | **rip** | **eigrp** [*as-number*]]

Syntax Description

as-number	(Optional) Clears the configuration commands for the specified EIGRP autonomous system number, also known as the process ID. If not specified, the configuration commands for all EIGRP routing processes are cleared. The range of values is 1 through 65535. Because only one EIGRP routing process is supported on the security appliance, including the optional *as-number* argument has the same effect as omitting it.
eigrp	(Optional) Specifies that only EIGRP router configuration commands are removed from the configuration. EIGRP interface configuration mode commands are not removed.
id	(Optional) Clears the configuration commands for the specified OSPF process ID. If not specified, the configuration commands for all OSPF processes are cleared.
ospf	(Optional) Specifies that only OSPF configuration commands are removed from the configuration.
rip	Specifies that only RIP configuration commands are removed from the configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was changed from the **clear router** command to the **clear configure router** command.
7.2(1)	The **rip** keyword was added to the command.
8.0(2)	The **eigrp** keyword was added to the command.

Examples

The following example clears all OSPF commands associated with OSPF process 1 from the running configuration:

```
hostname(config)# clear configure router ospf 1
```

The following example clears all global configuration mode commands associated with RIP routing process from the running configuration. It does not clear RIP commands entered in interface configuration mode.

```
hostname(config)# clear configure router rip
```

Related Commands

Command	Description
show running-config router	Displays the commands in the global router configuration.
router eigrp	Enables an EIGRP routing process and enters router configuration mode for that process.
router ospf	Enables an OSPF routing process and enters router configuration mode for that process.
router rip	Enables a RIP routing process and enters router configuration mode for that process.

clear configure same-security-traffic

To clear the same-security-traffic configuration, use the **clear configure same-security-traffic** command in global configuration mode.

clear configure same-security-traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the configuration when the **same-security-traffic** command is issued.:

```
hostname(config)# clear configure same-security-traffic
```

Related Commands

Command	Description
same-security-traffic	Permits communication between interfaces with equal security levels.
show running-config same-security-traffic	Displays the configuration when the **same-security-traffic** command is issued.

clear configure service-policy

To clear the service policy configuration, use the **clear configure service-policy** command in global configuration mode.

clear configure service-policy

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is an example of the **clear configure service-policy** command:

```
hostname(config)# clear configure service-policy
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
service-policy	Configures the service policy.
clear service-policy	Clears service policy statistics.

clear configure sla monitor

To remove the **sla monitor** commands from the running configuration, use the **clear configure sla monitor** command in global configuration mode.

clear configure sla monitor [*sla-id*]

Syntax Description

sla-id	(Optional) The ID of the SLA operation. Valid values are from 1 to 2147483647.

Defaults

If the *sla-id* is not specified, all SLA operation configurations are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command clears the **sla monitor** command, associated SLA monitor configuration mode commands, and the associated **sla monitor** schedule command, if present. It does not remove the **track rtr** commands from the configuration.

To view the sla monitor commands in the running configuration, use the **show running-config sla monitor** command.

Examples

The following example clears all **sla monitor** commands from the configuration:

```
hostname(config)# clear configure sla monitor
```

The following example clears the **sla monitor** commands associated with the SLA operation ID 5:

```
hostname(config)# clear configure sla monitor 5
```

Related Commands

Command	Description
show running-config sla monitor	Displays the sla monitor commands in the running configuration.

clear configure smtps

To remove all SMTPS commands from the configuration, reverting to default values, use the **clear configure smtps** command in global configuration mode.

clear configure smtps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the SMTPS configuration:

```
hostname(config)# clear configure smtps
```

Related Commands

Command	Description
show running-configuration smtps	Displays the running configuration for SMTPS.
smtps	Creates or edits an SMTPS e-mail proxy configuration.

clear configure smtp-server

To clear all of the SMTP server commands and statistics, use the **clear configure smtp-server** command in global configuration mode.

clear configure smtp-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	Support for this command was introduced.

Usage Guidelines

The **clear configure smtp-server** command clears all of the **smtp** commands and statistical information.

Examples

The following example shows how to clear all **smtp-server** commands:

```
hostname(config)# clear configure smtp-server
```

Related Commands

Command	Description
show running-config smtp-server	Displays the current DHCP server configuration.

clear configure snmp-map

To clear the SNMP map configuration, use the **clear configure snmp-map** command in global configuration mode.

clear configure snmp-map

Syntax DescriptionT

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure snmp-map** command removes the SNMP map configuration.

Examples

The following example clears the SNMP map configuration:

```
hostname# clear configure snmp-map
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enable SNMP application inspection.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.

clear configure snmp-server

To disable the SNMP server, use the **clear configure snmp-server** command in global configuration mode.

clear configure snmp-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to disable the SNMP server:

```
hostname# clear configure snmp-server
```

Related Commands

Command	Description
snmp-server	Provides the security appliance event information through SNMP.
show snmp-server statistics	Displays information about the SNMP server configuration.

clear configure ssh

To clear all SSH commands from the running configuration, use the **clear configure ssh** command in global configuration mode.

clear configure ssh

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **clear ssh** command to the **clear configure ssh** command.

Usage Guidelines

This command clears all SSH commands from the configuration. To clear specific commands, use the **no** form of those commands.

Examples

The following example clears all SSH commands from the configuration:

```
hostname(config)# clear configure ssh
```

Related Commands

Command	Description
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

clear configure ssl

To remove all SSL commands from the configuration, reverting to default values, use the **clear configure ssl** command in global configuration mode.

clear configure ssl

Syntax Description

This command has no arguments or keywords.

Defaults

By default:

- Both the SSL client and SSL server versions are **any**.
- SSL encryption is 3des-sha1 | des-sha1 | rc4-md5, in that order.
- There is no trust point association; the security appliance uses the default RSA key-pair certificate.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to use the **clear configure ssl** command:

```
hostname(config)# clear configure ssl
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured ssl commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

clear configure static

To remove all the **static** commands from the configuration, use the **clear configure static** command in global configuration mode.

clear configure static

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **configure** was added.

Examples

This example shows how to remove all the **static** commands from the configuration:

```
hostname(config)# clear configure static
```

Related Commands

Command	Description
show running-config static	Displays all **static** commands in the configuration.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

clear configure sunrpc-server

To clear the remote processor call services from the security appliance, use the **clear configure sunrpc-server** command in global configuration mode.

clear configure sunrpc-server [**active**]

Syntax Description

active	(Optional) Identifies the SunRPC services that are currently active on the security appliance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **sunrpc-server** command displays the configured **router ospf** commands.

Note If the highest-level IP address on the security appliance is a private address, this address is sent in hello packets and database definitions. To prevent this action, set the **router-id** *ip_address* to a global address.

Examples

The following example shows how to clear the SunRPC services from the security appliance:

```
hostname(config)# clear configure sunrpc-server active
```

Related Commands

Command	Description
sunrpc-server	Creates the SunRPC services table.
show running-config sunrpc-server	Displays the information about the SunRPC configuration.

clear configure sysopt

To clear the configuration for all **sysopt** commands, use the **clear configure sysopt** command in global configuration mode.

clear configure sysopt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **clear sysopt**.

Examples

The following example clears all **sysopt** command configuration:

```
hostname(config)# clear configure sysopt
```

Related Commands

Command	Description
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

clear configure tcp-map

To clear tcp-map configuration, use the **clear configure tcp-map** command in global configuration mode.

clear configure tcp-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to clear the TCP map configuration:

```
hostname(config)# clear configure tcp-map
```

Related Commands

Command	Description
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.
show running-config tcp-map	Displays the information about the TCP map configuration.

clear configure telnet

To remove the Telnet connection and idle timeout from the configuration, use the **clear configure telnet** command in global configuration mode.

clear configure telnet

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **configure** was added.

Examples

This example shows how to remove the Telnet connection and the idle timeout from the security appliance configuration:

```
hostname(config)# clear configure telnet
```

Related Commands

Command	Description
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the security appliance.
telnet	Adds Telnet access to the console and sets the idle timeout.

clear configure terminal

To clear the terminal display width setting, use the **clear configure terminal** command in global configuration mode.

clear configure terminal

Syntax Description

This command has no keywords or arguments.

Defaults

The default display width is 80 columns.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The **configure** keyword was added.

Examples

The following example clears the display width:

```
hostname# clear configure terminal
```

Related Commands

Command	Description
terminal	Sets the terminal line parameters.
terminal width	Sets the terminal display width.
show running-config terminal	Displays the current terminal settings.

clear configure threat-detection

To clear the threat detection configuration, use the **clear configure threat-detection** command in global configuration mode.

clear configure threat-detection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command clears all **threat-detection** configuration commands.

Examples

The following example clears all threat detection commands:

```
hostname# clear configure threat-detection
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
clear threat-detection shun	Releases currently shunned hosts.
show running-config threat-detection	Shows the threat detection configuration.
threat-detection basic-threat	enables basic threat detection.
threat-detection scanning-threat	Enables scanning threat detection.

clear configure timeout

To restore the default idle time durations in the configuration, use the **clear configure timeout** command in global configuration mode.

clear configure timeout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to remove the maximum idle time durations from the configuration:

```
hostname(config)# clear configure timeout
```

Related Commands

Command	Description
show running-config timeout	Displays the timeout value of the designated protocol.
timeout	Sets the maximum idle time duration.

clear configure time-range

To clear all configured time ranges, use the **clear configure time-range** command in global configuration mode.

clear configure time-range

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears all configured time ranges:

```
hostname(config)# clear configure time-range
```

Related Commands

Command	Description
time-range	Enters time-range configuration mode and defines a time range that you can attach to traffic rules, or an action.

clear configure tls-proxy

To remove all configured TLS proxy instances, use the **clear configure tls-proxy** command in global configuration mode.

clear configure tls-proxy

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following following example removes all configured TLS proxy instances using the **clear configure tls-proxy** command:

```
hostname# clear configure tls-proxy
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show running-config tls-proxy	Shows running configuration of all or specified TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

clear configure tunnel-group

To remove all or specified tunnel groups from the configuration, use the **clear config tunnel-group** command in global configuration.

clear config tunnel-group [*name*]

Syntax Description

name	(Optional) Specifies the name of a tunnel group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, removes the toengineering tunnel group from the configuration:

```
hostname(config)# clear config tunnel-group toengineering
hostname(config)#
```

Related Commands

Command	Description
show running-config tunnel-group	Displays information about all or selected tunnel-groups.
tunnel-group	Enters tunnel-group subconfiguration mode for the specified type.

clear configure tunnel-group-map

The **clear configure tunnel-group-map** command clears the policy and rules by which the tunnel-group name is derived from the content of the certificate.

clear configure tunnel-group-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The tunnel-group-map commands configure the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. To associate the certificate map entries, created using the **crypto ca certificate map** command, with tunnel groups, use the **tunnel-group-map** command in global configuration mode. You can invoke this command multiple times as long as each invocation is unique and you do not reference a map index more than once.

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

The processing that derives the tunnel-group name from the certificate ignores entries in the certificate map that are not associated with a tunnel group (any map rule not identified by this command).

Examples

The following example entered in global configuration mode, specifies a default tunnel group to use when the name cannot be derived by other configured methods. The name of the tunnel group to use is group1:

```
hostname(config)# clear configure tunnel-group-map
```

Related Commands

Command	Description
crypto ca certificate map	Enters crypto ca certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.
tunnel-group-map enable	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

clear configure url-block

To clear clears URL pending block buffer and long URL support configuration, use the **clear configure url-block** command in global configuration mode.

clear configure url-block

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure url-block** command clears URL pending block buffer and long URL support configuration.

Examples

The following example clears URL pending block buffer and long URL support configuration:

```
hostname# clear configure url-block
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear configure url-cache

To clear the URL cache, use the **clear configure url-cache** command in global configuration mode.

clear configure url-cache

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure url-cache** command clears the URL cache.

Examples

The following example clears the URL cache:

```
hostname# clear configure url-cache
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **scsc** command.

clear configure url-list

To remove a configured set of URLs that WebVPN users can access , use the **clear configure url-list** command in global configuration mode. To remove all configured URLs, use this command without the *listname* argument. To remove only the URLs for a specific list, use this command with that *listname*.

clear configure url-list [*listname***]**

Syntax Description

listname	Groups the set of URLs WebVPN users can access. Maximum 64 characters.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the URL list called *Marketing URLs*.

```
hostname(config)# clear configure url-list Marketing URLs
```

Related Commands

Command	Description
show running-configuration url-list	Displays the current set of configured **url-list** commands.
url-list	Use this command in global configuration mode to configure the set of URLs that WebVPN users can access.
url-list	Use this command in webvpn mode that you access from group-policy or username mode to enable WebVPN URL access for a specific group policy or user.

clear configure url-server

To clear the URL filtering server configuration, use the **clear configure url-server** command in global configuration mode.

clear configure url-server

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure url-server** command clears the URL filtering server configuration.

Examples

The following example URL filtering server configuration:

```
hostname# clear configure url-server
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear configure username

To clear the username database, use the **clear configure username** command in global configuration mode. To clear the configuration for a particular user, use this command and append the username.

clear configure username [*name***]**

Syntax Description

name	(Optional) Provides the name of the user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The internal user authentication database consists of the users entered with the username command. The login command uses this database for authentication.

Examples

The following example shows how to clear the configuration for the user named anyuser:

```
hostname(config)# clear configure username anyuser
```

Related Commands

Command	Description
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the security appliance database.
username attributes	Lets you configure AVPs for specific users.

clear configure virtual

To remove the authentication virtual server from the configuration, use the **clear configure virtual** command in global configuration mode.

clear configure virtual

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

There is no undo.

Examples

This example shows the **clear configure virtual** command:

```
hostname(config)# clear configure virtual
```

Related Commands

Command	Description
show running-config virtual	Displays the IP address for the authentication virtual server.
virtual http	Allows separate authentication with the security appliance and with the HTTP server.
virtual telnet	Authenticates users with the virtual Telnet server for traffic types for which the security appliance does not supply an authentication prompt.

clear configure vpdn group

To remove all **vpdn group** commands from the configuration, use the **clear configure vpdn group** command in global configuration mode.

clear configure vpdn group

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Entering the **clear configure vpdn group** command has no affect upon active PPPoE connections.

Examples

The following example shows how to clear the vpdn group configuration:

```
hostname(config)# clear configure vpdn group
```

Related Commands

Command	Description
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show running-config vpdn username	Shows the current configuration for vpdn usernames.

clear configure vpdn username

To remove all **vpdn username** commands from the configuration, use the **clear configure vpdn username** command in global configuration mode.

clear configure vpdn username

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Entering the **clear configure vpdn username** command has no affect upon active PPPoE connections.

Examples

The following example shows how to clear the vpdn username configuration:

```
hostname(config)# clear configure vpdn username
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configuration.
show running-config vpdn username	Shows the current configuration for vpdn usernames.

clear configure vpn-load-balancing

To remove the previously specified VPN load-balancing configuration, thus disabling VPN load-balancing, use the **clear configure vpn load-balancing** command in global configuration mode.

clear configure vpn load-balancing

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear configure vpn load-balancing** command also clears the following related commands: **cluster encryption**, **cluster ip address**, **cluster key**, **cluster port**, **nat**, **participate**, and **priority**.

Examples

The following command removes vpn load-balancing configuration statements from the configuration:

```
hostname(config)# clear configure vpn load-balancing
```

Related Commands

show running-config load-balancing	Displays the current VPN load-balancing configuration.
vpn load-balancing	Enters vpn load-balancing mode.

clear configure wccp

To remove all WCCP configuration, use the **clear configure wccp** command in global configuration mode.

clear configure wccp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to clear the WCCP configuration:

```
hostname(config)# clear configure wccp
```

Related Commands

Command	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

clear configure zonelabs-integrity

To remove all Zone Labs Integrity Servers from the running configuration, use the **clear configure zonelabs-integrity** command in global configuration mode.

clear configure zonelabs-integrity

Syntax Description

This command has no arguments or keywords.

Defaults

Remove all Zone Lab Integrity Servers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2.(1)	This command was introduced.

Usage Guidelines

The **clear configure zonelabs-integrity** command removes all Zone Labs Integrity Servers from the running configuration including active and standby Integrity servers.

Examples

The following example shows the removal of two configured Zone Labs Integrity Servers:

```
hostname(config)# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
hostname(config)# clear configure zonelabs-integrity
hostname(config)# show running-config zonelabs-integrity
hostname(config)#
```

Related Commands

Command	Description
show running-config [all] zonelabs-integrity	Display the configured Zone Labs Integrity Servers.

CHAPTER 7

clear conn through clear xlate Commands

clear conn

To clear a specific connection or multiple connections, use the **clear conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

clear conn [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[-*src_ip*] [**netmask** *mask*]]
[**port** *src_port*[-*src_port*]] [**address** *dest_ip*[-*dest_ip*] [**netmask** *mask*]]
[**port** *dest_port*[-*dest_port*]]

Syntax Description

address	(Optional) Clears connections with the specified source or destination IP address.
all	(Optional) Clears all connections that are to the device or from the device, in addition to through-traffic connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Clears connections with the specified source or destination port.
protocol {tcp | udp}	(Optional) Clears connections with the protocol **tcp** or **udp**.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

When the security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

Examples

The following example shows all connections, and then clears the management connection between 10.10.10.108:4168 and 10.0.8.112:22:

```
hostname# show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00, bytes 3084, flags
UOB

hostname# clear conn address 10.10.10.108 port 4168 address 10.0.8.112 port 22
```

Related Commandss

Commands	Description
clear local-host	Clears all connections by a specific local host or all local hosts.
clear xlate	Clears a NAT session, and any connections using NAT.
show conn	Shows connection information.
show local-host	Displays the network states of local hosts.
show xlate	Shows NAT sessions.

clear console-output

To remove the currently captured console output, use the **clear console-output** command in privileged EXEC mode.

clear console-output

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to remove the currently captured console output:

```
hostname# clear console-output
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the security appliance.
show console-output	Displays the captured console output.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

clear counters

To clear the protocol stack counters, use the **clear counters** command in global configuration mode.

clear counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

Syntax Description

all	(Optional) Clears all filter details.
context *context-name*	(Optional) Specifies the context name.
:*counter_name*	(Optional) Specifies a counter by name.
detail	(Optional) Clears detailed counters information.
protocol *protocol_name*	(Optional) Clears the counters for the specified protocol.
summary	(Optional) Clears the counter summary.
threshold *N*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

The **clear counters summary detail** is the default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows how to clear the protocol stack counters:

```
hostname(config)# clear counters
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

clear crashinfo

To delete the contents of the crash file in Flash memory, use the **clear crashinfo** command in privileged EXEC mode.

clear crashinfo

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following command shows how to delete the crash file:

```
hostname# clear crashinfo
```

Related Commands

crashinfo force	Forces a crash of the security appliance.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file stored in Flash memory.

clear crypto accelerator statistics

To clear the the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in privileged EXEC mode.

clear crypto accelerator statistics

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays crypto accelerator statistics:

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

Related Commands

Command	Description
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear crypto ca crls

To remove the CRL cache of all CRLs associated with a specified trustpoint or to remove the CRL cache of all CRLs, use the **clear crypto ca crls** command in privileged EXEC mode.

clear crypto ca crls [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command clears all CRLs cached on the system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example issued in global configuration mode, removes all of the CRL cache from all CRLs from the security appliance:

```
hostname# clear crypto ca crls
hostname#
```

Related Commands

Command	Description
crypto ca crl request	Downloads the CRL based on the CRL configuration of the trustpoint.
show crypto ca crls	Displays all cached CRLs or CRLs cached for a specified trustpoint.

clear crypto ipsec sa

To remove the IPSec SA counters, entries, crypto maps or peer connections, use the **clear crypto ipsec sa** command in privileged EXEC mode. To clear all IPSec SAs, use this command without arguments.

clear [crypto] ipsec sa [counters | entry {*hostname* | *ip_address***} {esp | ah}** *spi* **| map** *map name* **| peer {***hostname* | *ip_address***}]**

Be careful when using this command.

Syntax Description

ah	Authentication header.
counters	Clears all IPSec per SA statistics.
entry	Deletes the tunnel that matches the specified IP address/hostname, protocol and SPI value.
esp	Encryption security protocol.
hostname	Identified a hostname assigned to an IP address.
ip_address	Identifies an IP address.
map	Deletes all tunnels associated with the specified crypto map as identified by map name.
map name	An alphanumeric string that identifies a crypto map. Max 64 characters.
peer	Deletes all IPSec SAs to a peer as identified by the specified hostname or IP address.
spi	Identifies the Security Parameters Index (a hexidecimal number).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, issued in global configuration mode, removes all of the IPSec SAs from the security appliance:

```
hostname# clear crypto ipsec sa
hostname#
```

The next example, issued in global configuration mode, deletes SAs with a peer IP address of 10.86.1.1.

```
hostname# clear crypto ipsec peer 10.86.1.1
hostname#
```

Related Commands

Command	Description
clear configure crypto map	Clears all or specified crypto maps from the configuration.
clear configure isakmp	Clears all ISAKMP policy configuration.
show ipsec sa	Displays information about IPSec SAs, including counters, entry, map name, peer IP address and hostname.
show running-config crypto	Displays the entire crypto configuration, including IPSec, crypto maps, dynamic crypto maps, and ISAKMP.

clear crypto protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in privileged EXEC mode.

clear crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which you want to clear statistics. Protocol choices are as follows: • **ikev1**—Internet Key Exchange version 1. • **ipsec**—IP Security Phase-2 protocols. • **ssl**—Secure Socket Layer. • **other**—Reserved for new protocols. • **all**—All protocols currently supported. In online help for this command, other protocols may appear that will be supported in future releases.

Defaults

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, clears all crypto accelerator statistics:

```
hostname# clear crypto protocol statistics all
hostname#
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.

Command	Description
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics in the crypto accelerator MIB.

clear dhcpd

To clear the DHCP server bindings and statistics, use the **clear dhcp** command in privileged EXEC mode.

clear dhcpd {**binding** [*ip_address*] | **statistics**}

Syntax Description

binding	Clears all the client address bindings.
ip_address	(Optional) Clears the binding for the specified IP address.
statistics	Clears statistical information counters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you include the optional IP address in the **clear dhcpd binding** command, only the binding for that IP address is cleared.

To clear all of the DHCP server commands, use the **clear configure dhcpd** command.

Examples

The following example shows how to clear the **dhcpd** statistics:

```
hostname# clear dhcpd statistics
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show dhcpd	Displays DHCP binding, statistic, or state information.

clear dhcprelay statistics

To clear the DHCP relay statistic counters, use the **clear dhcprelay statistics** command in privileged EXEC mode.

clear dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear dhcprelay statistics** command only clears the DHCP relay statistic counters. To clear the entire DHCP relay configuration, use the **clear configure dhcprelay** command.

Examples

The following example shows how to clear the DHCP relay statistics:

```
hostname# clear dhcprelay statistics
hostname#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

clear dns-hosts cache

To clear the DNS cache, use the **clear dns-hosts cache** command in privileged EXEC mode. This command does not clear static entries you added with the **name** command.

clear dns-hosts cache

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the DNS cache:

```
hostname# clear dns-hosts cache
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

clear eigrp events

To clear the EIGRP event log, use the **clear eigrp events** command in privileged EXEC mode.

clear eigrp [*as-number*] **events**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **show eigrp events** command to view the EIGRP event log.

Examples

The following example clears the EIGRP event log:

```
hostname# clear eigrp events
```

Related Commands

Command	Description
show eigrp events	Displays the EIGRP event log.

clear eigrp neighbors

To delete entries from the EIGRP neighbor table, use the **clear eigrp neighbors** command in privileged EXEC mode.

clear eigrp [*as-number*] **neighbors** [*ip-addr* | *if-name*] [**soft**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name removes all neighbor table entries that were learned through this interface.
ip-addr	(Optional) The IP address of the neighbor you want to remove from the neighbor table.
soft	Causes the security appliance to resynchronize with the neighbor without resetting the adjacency.

Defaults

If you do not specify a neighbor IP address or an interface name, all dynamic entries are removed from the neighbor table.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **clear eigrp neighbors** command does not remove neighbors defined using the **neighbor** command from the neighbor table. Only dynamically-discovered neighbors are removed.

You can use the **show eigrp neighbors** command to view the EIGRP neighbor table.

Examples

The following example removes all entries from the EIGRP neighbor table:

```
hostname# clear eigrp neighbors
```

The following example removes all entries learned through the interface named “outside” from the EIGRP neighbor table:

```
hostname# clear eigrp neighbors outside
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debug information for EIGRP neighbors.
debug ip eigrp	Displays debug information for EIGRP protocol packets.
show eigrp neighbors	Displays the EIGRP neighbor table.

clear eigrp topology

To delete entries from the EIGRP topology table, use the **clear eigrp topology** command in privileged EXEC mode.

clear eigrp [*as-number*] **topology** *ip-addr* [*mask*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number (process ID).
ip-addr	The IP address to clear from the topology table.
mask	(Optional) The network mask to apply to the *ip-addr* argument.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command clears existing EIGRP entries from the EIGRP topology table. You can use the **show eigrp topology** command to view the topology table entries.

Examples

The following example removes entries in the 192.168.1.0 network from EIGRP topology table:

```
hostname# clear eigrp topology 192.168.1.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

clear failover statistics

To clear the failover statistic counters, use the **clear failover statistics** command in privileged EXEC mode.

clear failover statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was introduced.

Usage Guidelines

This command clears the statistics displayed with the **show failover statistics** command and the counters in the Stateful Failover Logical Update Statistics section of the **show failover** command output. To remove the failover configuration, use the **clear configure failover** command.

Examples

The following example shows how to clear the failover statistic counters:

```
hostname# clear failover statistics
hostname#
```

Related Commands

Command	Description
debug fover	Displays failover debug information.
show failover	Displays information about the failover configuration and operational statistics.

clear fragment

To clear the operational data of the IP fragment reassembly module, enter the **clear fragment** command in privileged EXEC mode. This command clears either the currently queued fragments that are waiting for reassembly (if the **queue** keyword is entered) or clears all IP fragment reassembly statistics (if the **statistics** keyword is entered). The statistics are the counters, which tell how many fragments chains were successfully reassembled, how many chains failed to be reassembled, and how many times the maximum size was crossed resulting in overflow of the buffer.

clear fragment {**queue** | **statistics**} [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.
queue	Clears the IP fragment reassembly queue.
statistics	Clears the IP fragment reassembly statistics.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **clear fragment** and **clear configure fragment**, to separate clearing of the configuration data from the operational data.

Examples

This example shows how to clear the operational data of the IP fragment reassembly module:

```
hostname# clear fragment queue
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

clear gc

To remove the garbage collection process statistics, use the **clear gc** command in privileged EXEC mode.

clear gc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to remove the garbage collection process statistics:

```
hostname# clear gc
```

Related Commands

Command	Description
show gc	Displays the garbage collection process statistics.

clear igmp counters

To clear all IGMP counters, use the **clear igmp counters** command in privileged EXEC mode.

clear igmp counters [*if_name*]

Syntax Description

if_name	The interface name, as specified by the **nameif** command. Including an interface name with this command causes only the counters for the specified interface to be cleared.

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the IGMP statistical counters:

```
hostname# clear igmp counters
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp group

To clear discovered groups from the IGMP group cache, use the **clear igmp** command in privileged EXEC mode.

clear igmp group [*group* | **interface** *name*]

Syntax Description

group	IGMP group address. Specifying a particular group removes the specified group from the cache.
interface *name*	Interface name, as specified by the **namif** command. When specified, all groups associated with the interface are removed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you do not specify a group or an interface, all groups are cleared from all interfaces. If you specify a group, only the entries for that group are cleared. If you specify an interface, then all groups on that interface are cleared. If you specify both a group and an interface, only the specified groups on the specified interface are cleared.

This command does not clear statically configured groups.

Examples

The following example shows how to clear all discovered IGMP groups from the IGMP group cache:

```
hostname# clear igmp group
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP counters.
clear igmp traffic	Clears the IGMP traffic counters.

clear igmp traffic

To clear the IGMP traffic counters, use the **clear igmp traffic** command in privileged EXEC mode.

clear igmp traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the IGMP statistical traffic counters:

```
hostname# clear igmp traffic
```

Related Commands

Command	Description
clear igmp group	Clears discovered groups from the IGMP group cache.
clear igmp counters	Clears all IGMP counters.

clear interface

To clear interface statistics, use the **clear interface** command in privileged EXEC mode.

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

By default, this command clears all interface statistics.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the security appliance clears only statistics for the current context. If you enter this command in the system execution space, the security appliance clears the combined statistics.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following example clears all interface statistics:

```
hostname# clear interface
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Displays the interface configuration.

clear ip audit count

To clear the count of signature matches for an audit policy, use the **clear ip audit count** command in privileged EXEC mode.

clear ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Clears the number of matches for all interfaces.
interface *interface_name*	(Optional) Clears the number of matches for the specified interface.

Defaults

If you do not specify a keyword, this command clears the matches for all interfaces (**global**).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the count for all interfaces:

```
hostname# clear ip audit count
```

Related Commands

Command	Description
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show ip audit count	Shows the count of signature matches for an audit policy.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

clear ip verify statistics

To clear the Unicast RPF statistics, use the **clear ip verify statistics** command in privileged EXEC mode. See the **ip verify reverse-path** command to enable Unicast RPF.

clear ip verify statistics [**interface** *interface_name*]

Syntax Description

interface *interface_name*	Sets the interface on which you want to clear Unicast RPF statistics.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example clears the Unicast RPF statistics:

```
hostname# clear ip verify statistics
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

clear ipsec sa

To clear IPSec SAs entirely or based on specified parameters, use the **clear ipsec sa** command in privileged EXEC mode. You can also use an alternate form: **clear crypto ipsec sa**.

clear ipsec sa [**counters | entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

Syntax Description

counters	(Optional) Clears all counters.
entry	(Optional) Clears IPSec SAs for a specified IPSec peer, protocol and SPI.
map *map-name*	(Optional) Clears IPSec SAs for the specified crypto map.
peer	(Optional) Clears IPSec SAs for a specified peer.
peer-addr	Specifies the IP address of an IPSec peer.
protocol	Specifies an IPSec protocol: **esp** or **ah**.
spi	Specifies an IPSec SPI.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, clears all IPSec SA counters:

```
hostname# clear ipsec sa counters
hostname#
```

Related Commands

Command	Description
show ipsec sa	Displays IPSec SAs based on specified parameters.
show ipsec stats	Displays global IPSec statistics from the IPSec flow MIB.

clear ipv6 access-list counters

To clear the IPv6 access list statistical counters, use the **clear ipv6 access-list counters** command in privileged EXEC mode.

clear ipv6 access-list *id* **counters**

Syntax Description

id	The IPv6 access list identifier.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to clear the statistical data for the IPv6 access list 2:

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

Related Commands

Command	Description
clear configure ipv6	Clears the **ipv6 access-list** commands from the current configuration.
ipv6 access-list	Configures an IPv6 access list.
show ipv6 access-list	Displays the **ipv6 access-list** commands in the current configuration.

clear ipv6 mld traffic

To clear the IPv6 Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

clear ipv6 mld traffic

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

The **clear ipv6 mld traffic** command allows you to reset all the Multicast Listener Discovery traffic counters.

Examples

The following example shows how to clear the traffic counters for the IPv6 Multicast Listener Discovery:

```
hostname# clear ipv6 mld traffic
hostname#
```

Related Commands

Command	Description
debug ipv6 mld	Displays all debug messages for Multicast Listener Discovery.
show debug ipv6 mld	Displays the **ipv6** Multicast Listener Discovery commands in the current configuration.

clear ipv6 neighbors

To clear the IPv6 neighbor discovery cache, use the **clear ipv6 neighbors** command in privileged EXEC mode.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command deletes all discovered IPv6 neighbor from the cache; it does not remove static entries.

Examples

The following example deletes all entries, except static entries, in the IPv6 neighbor discovery cache:

```
hostname# clear ipv6 neighbors
hostname#
```

Related Commands

Command	Description
ipv6 neighbor	Configures a static entry in the IPv6 discovery cache.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

clear ipv6 traffic

To reset the IPv6 traffic counters, use the **clear ipv6 traffic** command in privileged EXEC mode.

clear ipv6 traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using this command resets the counters in the output from the **show ipv6 traffic** command.

Examples

The following example resets the IPv6 traffic counters. The output from the **ipv6 traffic** command shows that the counters are reset:

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
```

```
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

Related Commands

Command	Description
show ipv6 traffic	Displays IPv6 traffic statistics.

clear isakmp sa

To remove all of the IKE runtime SA database, use the **clear isakmp sa** command in global configuration or privileged EXEC mode.

clear isakmp sa

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **clear isakmp sa** command was changed to **clear crypto isakmp sa**.

Examples

The following example removes the IKE runtime SA database from the configuration:

```
hostname# clear isakmp sa
hostname#
```

Related Commands

Command	Description
clear isakmp	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp stats	Displays runtime statistics.
show isakmp sa	Displays IKE runtime SA database with additional information.
show running-config isakmp	Displays all the active ISAKMP configuration.

clear local-host

To release network connections from local hosts displayed by entering the **show local-host** command, use the **clear local-host** command in privileged EXEC mode.

clear local-host [*ip_address*] [**all**]

Syntax Description

all	(Optional) Specifies to clear the local hosts state-made connections, including to the security appliance and from the security appliance.
ip_address	(Optional) Specifies the local host IP address.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear local-host** command releases the cleared hosts from the license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Caution Clearing the network state of a local host stops all network connections and xlates that are associated with the local hosts.

Examples

The following example shows how the **clear local-host** command clears the information about the local hosts:

```
hostname# clear local-host 10.1.1.15
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

Command	Description
show local-host	Displays the network states of local hosts.

clear logging asdm

To clear the ASDM logging buffer, use the **clear logging asdm** command in privileged EXEC mode.

clear logging asdm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **clear pdm logging** command to the **clear asdm log** command.

Usage Guidelines

ASDM system log messages are stored in a separate buffer from the security appliance system log messages. Clearing the ASDM logging buffer only clears the ASDM system log messages; it does not clear the security appliance system log messages. To view the ASDM system log messages, use the **show asdm log** command.

Examples

The following example clears the ASDM logging buffer:

```
hostname(config)# clear logging asdm
hostname(config)#
```

Related Commands

Command	Description
show asdm log_sessions	Displays the contents of the ASDM logging buffer.

clear logging queue

To clear logging-related queues, use the **clear logging queue** command in privileged EXEC mode.

clear logging queue [bufferwrap]

Syntax Description

bufferwrap	Clears the FTP and flash logging buffer.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(5)	This command was introduced.

Examples

The following example shows how to clear the FTP and flash logging buffer:

```
hostname# clear logging queue bufferwrap
```

Related Commands

Command	Description
logging buffered	Configures the logging buffer.
show logging	Displays logging information.

clear mac-address-table

To clear dynamic MAC address table entries, use the **clear mac-address-table** command in privileged EXEC mode.

clear mac-address-table [*interface_name*]

Syntax Description

interface_name	(Optional) Clears the MAC address table entries for the selected interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the dynamic MAC address table entries:

```
hostname# clear mac-address-table
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

clear memory delayed-free-poisoner

To clear the delayed free-memory poisoner tool queue and statistics, use the **clear memory delayed-free-poisoner** command in privileged EXEC mode.

clear memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear memory delayed-free-poisoner** command returns all memory held in the delayed free-memory poisoner tool queue to the system without validation and clears the related statistical counters.

Examples

The following example clears the delayed free-memory poisoner tool queue and statistics:

```
hostname# clear memory delayed-free-poisoner
```

Related Commands

Command	Description
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

clear memory profile

To clear the memory buffers held by the memory profiling function, use the **clear memory profile** command in privileged EXEC mode.

clear memory profile [peak]

Syntax Description

peak	(Optional) Clears the contents of the peak memory buffer.

Defaults

Clears the current "in use" profile buffer by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **clear memory profile** command releases the memory buffers held by the profiling function and therefore requires that profiling stop before it is cleared.

Examples

The following example clears the memory buffers held by the profiling function:

```
hostname# clear memory profile
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.

clear mfib counters

To clear MFIB router packet counters, use the **clear mfib counters** command in privileged EXEC mode.

clear mfib counters [*group* [*source*]]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

When this command is used with no arguments, route counters for all routes are cleared.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears all MFIB router packet counters:

```
hostname# clear mfib counters
```

Related Commands

Command	Description
show mfib count	Displays MFIB route and packet count data.

clear module recover

To clear the AIP SSM recovery network settings set in the **hw-module module recover** command, use the **clear module recover** command in privileged EXEC mode.

clear module 1 recover

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the recovery settings for the AIP SSM:

```
hostname# clear module 1 recover
```

Related Commands

Command	Description
hw-module module recover	Recovers an AIP SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the AIP SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

clear nac-policy

To reset NAC policy usage statistics, use the **clear nac-policy** command in global configuration mode.

clear nac-policy [*nac-policy-name***]**

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to reset usage statistics.

Defaults

If you do not specify a name, the CLI resets the usage statistics for all NAC policies.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following command resets the usage statistics for the NAC policy named framework1:

```
hostname(config)# clear nac-policy framework1
```

The following command resets all NAC policy usage statistics:

```
hostname(config)# clear nac-policy
```

Related Commands

Command	Description
show nac-policy	Displays NAC policy usage statistics on the security appliance.
show vpn-session_summary.db	Displays the number IPSec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

clear nat counters

To clear NAT policy counters, use the **clear nat counters** command in global configuration mode.

clear nat counters [*src_if* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0 (4)	This command was introduced.

Examples

The following example shows how to clear the NAT policy counters:

```
hostname(config)# clear nat counters
```

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables/disables NAT configuration requirement.
show nat counters	Displays the protocol stack counters.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

clear ospf [*pid*] {**process** | **counters** [**neighbor** [*neighbor-intf*] [*neighbr-id*]]}

Syntax Description

counters	Clears the OSPF counters.
neighbor	Clears the OSPF neighbor counters.
neighbor-intf	(Optional) Clears the OSPF interface router designation.
neighbr-id	(Optional) Clears the OSPF neighbor router ID.
pid	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
process	Clears the OSPF routing process.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command does not remove any part of the configuration. Use the **no** form of the configuration commands to clear specific commands from the configuration or use the **clear configure router ospf** command to remove all global OSPF commands from the configuration.

Note The **clear configure router ospf** command does not clear OSPF commands entered in interface configuration mode.

Examples

The following example shows how to clear the OSPF process counters:

```
hostname# clear ospf process
```

Related Commands

Command	Description
clear configure router	Clears all global router commands from the running configuration.

clear pc

To clear connection, xlate, or local-host information maintained on the PC, use the **clear pc** command in privileged EXEC mode.

clear pc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears PC information:

```
hostname# clear pc
```

Related Commands

Command	Description
clear pclu	Clears PC logical update statistics.

clear pclu

To clear PC logical update statistics, use the **clear pclu** command in privileged EXEC mode.

clear pclu

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears PC information:

```
hostname# clear pclu
```

Related Commands

Command	Description
clear pc	Clears connection, xlate, or local-host information maintained on PC.

clear pim counters

To clear the PIM traffic counters, use the **clear pim counters** command in privileged EXEC mode.

clear pim counters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command only clears the traffic counters. To clear the PIM topology table, use the **clear pim topology** command.

Examples

The following example clears the PIM traffic counters:

```
hostname# clear pim counters
```

Related Commands

Command	Description
clear pim reset	Forces MRIB synchronization through reset.
clear pim topology	Clears the PIM topology table.
show pim traffic	Displays the PIM traffic counters.

clear pim reset

To force MRIB synchronization through reset, use the **clear pim reset** command in privileged EXEC mode.

clear pim reset

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

All information from the topology table is cleared and the MRIB connection is reset. This command can be used to synchronize state between the PIM topology table and the MRIB database.

Examples

The following example clears the topology table and resets the MRIB connection:

```
hostname# clear pim reset
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim topology	Clears the PIM topology table.
clear pim counters	Clears PIM traffic counters.

clear pim topology

To clear the PIM topology table, use the **clear pim topology** command in privileged EXEC mode.

clear pim topology [*group*]

Syntax Description

group	(Optional) Specifies the multicast group address or name to be deleted from the topology table.

Defaults

Without the optional *group* argument, all entries are cleared from the topology table.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as IGMP local membership, is retained. If a multicast group is specified, only those group entries are cleared.

Examples

The following example clears the PIM topology table:

```
hostname# clear pim topology
```

Related Commands

Command	Description
clear pim counters	Clears PIM counters and statistics.
clear pim reset	Forces MRIB synchronization through reset.
clear pim counters	Clears PIM traffic counters.

clear priority-queue statistics

To clear the priority-queue statistics counters for an interface or for all configured interfaces, use the **clear priority-queue statistics** command in either global configuration or privileged EXEC mode.

clear priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command clears the priority-queue statistics for all configured interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the **clear priority-queue statistics** command in privileged EXEC mode to remove the priority queue statistics for the interface named “test”.

```
hostname# clear priority-queue statistics test
hostname#
```

Related Commands

Command	Description
clear configure priority queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the priority queue statistics for a specified interface or for all interfaces.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

clear resource usage

To clear resource usage statistics, use the **clear resource usage** command in privileged EXEC mode.

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify **all** (the default) for all contexts.
resource [**rate**] *resource_name*	Clears the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to clear the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the security appliance. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—System log messages. • **telnet**—Telnet sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Clears the combined context statistics.
system	(Multiple mode only) Clears the system-wide (global) usage statistics.

Defaults

For multiple context mode, the default context is **all**, which clears resource usage for every context. For single mode, the context name is ignored and all resource statistics are cleared.

The default resource name is **all**, which clears all resource types.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears all resource usage statistics for all contexts, but not the system-wide usage statistics:

```
hostname# clear resource usage
```

The following example clears the system-wide usage statistics:

```
hostname# clear resource usage system
```

Related Commands

Command	Description
context	Adds a security context.
show resource types	Shows a list of resource types.
show resource usage	Shows the resource usage of the security appliance.

clear route

To remove dynamically learned routes from the configuration, use the **clear route** command in privileged EXEC mode.

clear route [*interface_name*]

Syntax Description

interface_name	(Optional) Internal or external network interface name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to remove dynamically learned routes:

```
hostname# clear route
```

Related Commands

Command	Description
route	Specifies a static or default route for the an interface.
show route	Displays route information.
show running-config route	Displays configured routes.

clear service-policy

To clear operational data or statistics (if any) for enabled policies, use the **clear service-policy** command in privileged EXEC mode. To clear service policy startistics for inspection engines, see the **clear service-policy inspect** commands.

clear service-policy [**global** | **interface** *intf*]

Syntax Description

global	(Optional) Clears the statistics of the global service policy.
interface *intf*	(Optional) Clears the service policy statistics of a specific interface.

Defaults

By default, this command clears all the statistics for all enabled service policies.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows the syntax of the **clear service-policy** command:

```
hostname# clear service-policy outside_security_map interface outside
```

Related Commands

Command	Description
clear service-policy inspect gtp	Clears service policy statistics for the GTP inspection engine.
clear service-policy inspect radius-accounting	Clears service policy statistics for the RADIUS accounting inspection engine.
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
clear configure service-policy	Clears service policy configurations.
service-policy	Configures service policies.

clear service-policy inspect gtp

To clear global GTP statistics, use the **clear service-policy inspect gtp** command in privileged EXEC mode.

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

Syntax Description.

all	Clears all GTP PDP contexts.
apn	(Optional) Clears the PDP contexts based on the APN specified.
ap_name	Identifies the specific access point name.
gsn	(Optional) Identifies the GPRS support node, which is the interface between the GPRS wireless data network and other networks.
gtp	(Optional) Clears the service policy for GTP.
imsi	(Optional) Clears the PDP contexts based on the IMSI specified.
IMSI_value	Hexadecimal value that identifies the specific IMSI.
interface	(Optional) Identifies a specific interface.
int	Identifies the interface for which information will be cleared.
IP_address	IP address for which statistics will be cleared.
ms-addr	(Optional) Clears PDP contexts based on the MS Address specified.
pdp-context	(Optional) Identifies the Packet Data Protocol context.
requests	(Optional) Clears GTP requests.
statistics	(Optional) Clears GTP statistics for the **inspect gtp** command.
tid	(Optional) Clears the PDP contexts based on the TID specified.
tunnel_ID	Hexadecimal value that identifies the specific tunnel.
version	(Optional) Clears the PDP contexts based on the GTP version.
version_num	Specifies the version of the PDP context. The valid range is 0 to 255.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The Packet Data Protocol context is identified by the tunnel ID, which is a combination of IMSI and NSAPI. A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station (MS) user.

Examples

The following example clears GTP statistics:

```
hostname# clear service-policy inspect gtp statistics
```

Related Commands

Commands	Description
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.
show running-config gtp-map	Shows the GTP maps that have been configured.

clear service-policy inspect radius-accounting

To clear RADIUS accounting users, use the **clear service-policy inspect radius-accounting** command in privileged EXEC mode.

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

Syntax Description.

all	Clears all users.
ip_address	Clears a user with this IP address.
policy_map	Clears users associated with this policy map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example clears all RADIUS users:

```
hostname# clear service-policy inspect radius-accounting users all
```

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command in privileged EXEC mode.

clear shun [*statistics*]

Syntax Description

statistics	(Optional) Clears the interface counters only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
hostname(config)# clear shun
```

Related Commands

Command	Description
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.
show shun	Displays the shun information.

clear startup-config errors

To clear configuration error messages from memory, use the **clear startup-config errors** command in privileged EXEC mode.

clear startup-config errors

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To view configuration errors generated when the security appliance loaded the startup configuration, use the **show startup-config errors** command.

Examples

The following example clears all configuration errors from memory:

```
hostname# clear startup-config errors
```

Related Commands

Command	Description
show startup-config errors	Shows configuration errors generated when the security appliance loaded the startup configuration.

clear sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the **clear sunrpc-server active** command in privileged EXEC mode.

clear sunrpc-server active

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **clear sunrpc-server active** command to clear the pinholes opened by Sun RPC application inspection that allow service traffic, such as NFS or NIS, to pass through the security appliance.

Examples

The following example shows how to clear the SunRPC services table:

```
hostname# clear sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.
show sunrpc-server active	Displays information about active Sun RPC services.

clear threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can clear statistics using the **clear threat detection rate** command in privileged EXEC mode.

clear threat-detection rate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example clears the rate statistics:

```
hostname# clear threat-detection rate
```

Related Commands

Command	Description
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command, then clear the attackers and targets using the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection scanning-threat [attacker [*ip_address* [*mask*]] |
target [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Clears a specific IP address .
mask	(Optional) Sets the subnet mask.
attacker	(Optional) Clears only attackers.
target	(Optional) Clears only targets.

Defaults

If you do not specify an IP address, all hosts are released.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To view current attackers and targets, use the **show threat-detection scanning-threat** command.

Examples

The following example shows targets and attackers with the **show threat-detection scanning-threat** command, and then clears all targets:

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
```

```
    192.168.10.7
    192.168.10.8
    192.168.10.9
hostname# clear threat-detection scanning-threat target
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command, and you automatically shun attacking hosts, then release the currently shunned hosts using the **clear threat-detection shun** command in privileged EXEC mode.

clear threat-detection shun [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Releases a specific IP address from being shunned.
mask	(Optional) Sets the subnet mask for the shunned host IP address.

Defaults

If you do not specify an IP address, all hosts are released.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To view currently shunned hosts, use the **show threat-detection shun** command.

Examples

The following example views currently shunned hosts with the **show threat-detection shun** command, and then releases host 10.1.1.6 from being shunned:

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
hostname# clear threat-detection shun 10.1.1.6 255.255.255.255
```

Related Commands

Command	Description
show threat-detection shun	Shows currently shunned hosts.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

clear threat-detection statistics

If you enable TCP Intercept statistics with the **threat-detection statistics tcp-intercept** command, then clear the statistics using the **clear threat-detection scanning-threat** command in privileged EXEC mode.

clear threat-detection statistics [tcp-intercept]

Syntax Description

tcp-intercept	(Optional) Clears TCP Intercept statistics. This is the default.

Defaults

Clears TCP Intercept statistics.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

To view TCP Intercept statistics, enter the **show threat-detection statistics top** command.

Examples

The following example shows TCP Intercept statistics with the **show threat-detection statistics top tcp-intercept** command, and then clears all statistics:

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

```
hostname# clear threat-detection statistics
```

Related Commands

Command	Description
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables threat detection statistics.

clear traffic

To reset the counters for transmit and receive activity, use the **clear traffic** command in privileged EXEC mode.

clear traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear traffic** command resets the counters for transmit and receive activity that is displayed with the **show traffic** command. The counters indicate the number of packets and bytes moving through each interface since the last clear traffic command was entered or since the security appliance came online. And the number of seconds indicate the duration the security appliance has been online since the last reboot.

Examples

The following example shows the **clear traffic** command:

```
hostname# clear traffic
```

Related Commands

Command	Description
show traffic	Displays the counters for transmit and receive activity.

clear uauth

To delete all the cached authentication and authorization information for a user or for all users, use the **clear uauth** command in privileged EXEC mode.

clear uauth [*username*]

Syntax Description

username	(Optional) Specifies, by username, the user authentication information to remove.

Defaults

Omitting username deletes the authentication and authorization information for all users.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear uauth** command deletes the AAA authorization and authentication caches for one user or for all users, which forces the user or users to reauthenticate the next time that they create a connection.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If the user attempts to access a service that has been cached from the correct host, the security appliance considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see the AAA commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows how to cause the user to reauthenticate:

```
hostname(config)# clear uauth user
```

Related Commands

Command	Description
aaa authentication	Enable, disable, or view LOCAL, TACACS+ or RADIUS user authentication (on a server designated by the **aaa-server** command).
aaa authorization	Enable, disable, or view TACACS+ or RADIUS user authorization (on a server designated by the **aaa-server** command).
show uauth	Display current user authentication and authorization information.
timeout	Set the maximum idle time duration.

clear url-block block statistics

To clear the block buffer usage counters, use the **clear url-block block statistics** command in privileged EXEC mode.

clear url-block block statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-block block statistics** command clears the block buffer usage counters, except for the `Current number of packets held (global)` counter.

Examples

The following example clears the URL block statistics and displays the status of the counters after clearing:

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
------------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
| exceeding url-block buffer limit: | 0
| HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear url-cache statistics

To remove **url-cache** command statements from the configuration, use the **clear url-cache** command in privileged EXEC mode.

clear url-cache statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-cache** command removes **url-cache** statistics from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enter the **| url-cache** command to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example clears the URL cache statistics:

```
hostname# clear url-cache statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear url-server

To clear URL filtering server statistics, use the **clear url-server** command in privileged EXEC mode.

clear url-server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear url-server** command removes URL filtering server statistics from the configuration.

Examples

The following example clears the URL server statistics:

```
hostname# clear url-server statistics
```

Related Commands

Commands	Description
filter url	Directs traffic to a URL filtering server.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

clear wccp

To reset WCCP information, use the **clear wccp** command in privileged EXEC mode.

clear wccp [**web-cache** | *service_number*]

Syntax Description

web-cache	Specifies the web-cache service.
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to reset the WCCP information for the web-cache service:

```
hostname# clear wccp web-cache
```

Related Commands

Command	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

clear webvpn sso-server statistics

To reset the statistics from the webvpn Single Sign-On (SSO) server, use the **clear webvpn sso-server statistics** command in privileged EXEC mode.

clear webvpn sso-server statistics *servername*

Syntax Description

servername	Specifies the name of the SSO server to be revoked.

Defaults

No default behavior or values.

Command Modes

The following table shows the mode in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This does not reset the "pending requests" statistic.

Examples

The following example entered in privileged EXEC mode, displays crypto accelerator statistics:

```
hostname # clear webvpn sso-server statistics
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

clear xlate

To clear current translation and connection information, use the **clear xlate** command in privileged EXEC mode.

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]] [**gport** *port1*[*-port2*]] [**lport** *port1*[*-port2*]] [**interface** *if_name*] [**state** *state*]

Syntax Description

global *ip1*[*-ip2*]	(Optional) Clears the active translations by global IP address or range of addresses.
gport *port1*[*-port2*]	(Optional) Clears the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1*[*-ip2*]	(Optional) Clears the active translations by local IP address or range of addresses.
lport *port1*[*-port2*]	(Optional) Clears the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Clears the active translations by state. You can enter one or more of the following states: • **static**—specifies **static** translations. • **portmap**—specifies PAT global translations. • **norandomseq**—specifies a **nat** or **static** translation with the **norondomseq** setting. • **identity**—specifies **nat 0** identity address translations. When specifying more than one state, separate the states with a space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots ("xlate" refers to the translation slot). Translation slots can persist after key changes have been made. Always use the **clear xlate** command after adding, changing, or removing the **aaa-server**, **access-list**, **alias**, **global**, **nat**, **route**, or **static** commands in your configuration.

An xlate describes a NAT or PAT session. These sessions can be viewed with the **show xlate** command with the **detail** option. There are two types of xlates: static and dynamic.

A static xlate is a persistent xlate that is created using the **static** command. The **clear xlate** command does not clear for a host in a static entry. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** command does not remove the static translation rule. If you remove a static command from the configuration, preexisting connections that use the static rule can still forward traffic. Use the **clear local-host** command to deactivate these connections.

A dynamic xlate is an xlate that is created on demand with traffic processing (through the **nat** or **global** command). The **clear xlate** command removes dynamic xlates and their associated connections. You can also use the **clear local-host** command to clear the xlate and associated connections. If you remove a **nat** or a **global** command from the configuration, the dynamic xlate and associated connections may remain active. Use the **clear xlate** command or the **clear local-host** command to remove these connections.

Examples

The following example shows how to clear the current translation and connection slot information:

```
hostname# clear xlate global
```

Related Commands

Command	Description
clear local-host	Clears local host network information.
clear uauth	Clears cached user authentication and authorization information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show xlate	Displays the current translation information.

CHAPTER 8

client access rule through crl configure Commands

client-access-rule

To configure rules that limit the remote access client types and versions that can connect via IPSec through the security appliance, use the **client-access-rule** command in group-policy configuration mode. To delete a rule, use the **no** form of this command.

To delete all rules, use the **no client-access-rule command** with only the priority argument. This deletes all configured rules, including a null rule created by issuing the **client-access-rule none** command.

When there are no client access rules, users inherit any rules that exist in the default group policy. To prevent users from inheriting client access rules, use the **client-access-rule none** command. The result of doing so is that all client types and versions can connect.

client-access-rule *priority* **{permit | deny} type** *type* **version** *version* **| none**

no client-access-rule *priority* [**{permit | deny} type** *type* **version** *version*]

Syntax Description

deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets client-access-rule to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the security appliance ignores it.
type *type*	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can use the * character as a wildcard.
version *version*	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can use the * character as a wildcard.

Defaults

By default, there are no access rules.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Construct rules according to these caveats:

- If you do not define any rules, the security appliance permits all connection types.
- When a client matches none of the rules, the security appliance denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the security appliance denies all connections.
- For both software and hardware clients, type and version must match exactly their appearance in the **show vpn-sessiondb remote** display.
- The * character is a wildcard, which you can use multiple times in each rule. For example, **client-access-rule 3 deny type * version 3.*** creates a priority 3 client access rule that denies all client types running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type and/or version.

Examples

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN Clients running software version 4.1, while denying all VPN 3002 hardware clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client (ctl-provider)

To specify clients allowed to connect to the Certificate Trust List provider, or to specify a username and password for client authentication, use the **client** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

Syntax Description

encrypted	Specifies encryption for the password.
interface *if_name*	Specifies the interface allowed to connect.
ipv4_addr	Specifies the IP address of the client.
username *user_name*	Specifies the username for client authentication.
password *password*	Specifies the password for client authentication.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **client** command in CTL provider configuration mode to specify the clients allowed to connect to the CTL provider, and to set the username and password for client authentication. More than one command may be issued to define multiple clients. The username and password must match the CCM Administrator's username and password for the CallManager cluster.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

client (tls-proxy)

To configure trustpoints, keypairs, and cipher suites, use the **client** command in TLS proxy configuration mode. To remove the configuration, use the **no** form of this command.

client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

Syntax Description

cipher-suite *cipher_suite*	Specifies the cipher suite. Options include des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.
issuer *ca_tp_name*	Specifies the local CA trustpoint to issue client dynamic certificates.
keypair *key_label*	Specifies the RSA keypair to be used by client dynamic certificates.
ldc	Specifies the local dynamic certificate issuer or keypair.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
TLS proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **client** command in TLS proxy configuration mode to control the TLS handshake parameters for the security appliance as the TLS client role in TLS proxy. This includes cipher suite configuration, or to set the local dynamic certificate issuer or keypair. The local CA to issue client dynamic certificates is defined by the **crypto ca trustpoint** command and the trustpoint must have **proxy-ldc-issuer** configured, or the default local CA server (LOCAL-CA-SERVER).

The keypair value must have been generated with the **crypto key generate** command.

For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suite replaces the default cipher suite, or the one defined by the **ssl encryption** command. You can use this command to achieve difference ciphers between the two TLS sessions. You should use AES ciphers with the CallManager server.

Examples

The following example shows how to create a TLS proxy instance:

```
hostname(config)# tls-proxy my_proxy
```

```
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

client-firewall

To set personal firewall policies that the security appliance pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, use the **no** form of this command.

To delete all firewall policies, use the **no client-firewall** command without arguments. This deletes all configured firewall policies, including a null policy created by issuing the **client-firewall none** command.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, use the **client-firewall none** command.

client-firewall none

client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

Note When the firewall type is **zonelabs-integrity**, do not include arguments. The Zone Labs Integrity Server determines the policies.

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl* }

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

Syntax Description

acl-in <*acl*>	Provides the policy the client uses for inbound traffic.
acl-out <*acl*>	Provides the policy the client uses for outbound traffic.
AYT	Specifies that the client PC firewall application controls the firewall policy. The security appliance checks to make sure the firewall is running. It asks, “Are You There?” If there is no response, the security appliance tears down the tunnel.
cisco-integrated	Specifies Cisco Integrated firewall type.
cisco-security-agent	Specifies Cisco Intrusion Prevention Security Agent firewall type.
CPP	Specifies Policy Pushed as source of the VPN Client firewall policy.
custom	Specifies Custom firewall type.

description <*string*>	Describes the firewall.
networkice-blackice	Specifies Network ICE Black ICE firewall type.
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing one. Prevents inheriting a firewall policy from a default or specified group policy.
opt	Indicates an optional firewall type.
product-id	Identifies the firewall product.
req	Indicates a required firewall type.
sygate-personal	Specifies Sygate Personal firewall type.
sygate-personal-pro	Specifies Sygate Personal Pro firewall type.
sygate-security-agent	Specifies Sygate Security Agent firewall type.
vendor-id	Identifies the firewall vendor.
zonelabs-integrity	Specifies Zone Labs Integrity Server firewall type.
zonelabs-zonealarm	Specifies Zone Labs Zone Alarm firewall type.
zonelabs-zonealarmorpro policy	Specifies Zone Labs Zone Alarm or Pro firewall type.
zonelabs-zonealarmpro policy	Specifies Zone Labs Zone Alarm Pro firewall type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **zonelabs-integrity** firewall type was added.

Usage Guidelines

Only one instance of this command can be configured.

Examples

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

To specify the proxy trustpoint certificate to be presented during TLS handshake when configuring the TLS Proxy for Cisco Unified Presence Server (CUPS), use the **client trust-point** command in tls-proxy configuration mode. To remove the proxy trustpoint certificate, use the **no** form of this command.

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint*]

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
TLS proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The **client trust-point** command specifies the trustpoint and associated certificate that the security appliance uses in the TLS handshake when the security appliance assumes the role of the TLS client. The certificate must be owned by the security appliance (identity certificate).

The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential. The **client trust-point** command has precedence over the global **ssl trust-point** command.

Examples

The following example shows the use of the client trust-point command to specify the use of trustpoint "ent_y_proxy" in the TLS handshake with the TLS server. The handshake is likely to be originated from entity Y to entity X where the TLS server resides. The ASA functions as the TLS proxy for entity Y.

```
hostname(config-tlsp)# client trust-point ent_y_proxy
```

Related Commands

Command	Description
client (tls-proxy)	Configures trustpoints, keypairs, and cipher suites for a TLS proxy instance.
server trust-point	Specifies the proxy trustpoint certificate to present during the TLS handshake when the security appliance assumes the role of the TLS server.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.
tls-proxy	Configures a TLS proxy instance.

client-types (crypto ca trustpoint)

To specify the client connection types for which this trustpoint can be used to validate the certificates associated with a user connection, use the **client-types command** in crypto ca trustpoint configuration mode. To specify that the trustpoint cannot be used for the named connection, use the **no** form of the command.

[no] client-types {ssl | ipsec}

Syntax Description

ipsec	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate IPSec connections.
ssl	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate SSL connections.

Defaults

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command History

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

When there are multiple trustpoints associated with the same CA certificate, only one of the trustpoints can be configured for a specific client type. However, one of the trustpoints can be configured for one client type and the other trustpoint with another client-type.

If there is a trustpoint associated with the same CA certificate that is already configured with a client type, the new trustpoint is not allowed to be configured with the same client-type setting. The no form of the command clears the setting so that trustpoint cannot be used for any client validation.

Remote-access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPSec), or both, depending on deployment requirements, to permit access to virtually any network application or resource.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint, central, and designates it an SSL trustpoint:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint, checkin1,anddesignated it as an IPsec trustpoint.

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

client-update

To issue a client-update for all active remote VPN software and hardware clients and security appliances configured as Auto Update clients, on all tunnel-groups or for a particular tunnel group, use the **client-update** command in privileged EXEC mode.

To configure and change client-update parameters at the global level, including VPN software and hardware clients and security appliances configured as Auto Update clients, use the **client-update** command in global configuration mode.

To configure and change client-update tunnel-group IPSec-attributes parameters for VPN software and hardware clients, use the **client-update** command in tunnel-group ipsec-attributes configuration mode.

If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update.

To disable a client update, use the **no** form of this command.

Global configuration mode command:

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

Tunnel-group ipsec-attributes mode command:

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

Privileged EXEC mode command:

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

Syntax Description

all	(Available only in privileged EXEC mode.) Applies the action to all active remote clients in all tunnel groups. You cannot use the keyword **all** with the **no** form of the command.
component {**asdm** | **image**}	The software component for security appliances configured as Auto Update clients.
device-id *dev_string*	If the Auto Update client is configured to identify itself with a unique string, specify the same string that the client uses. The maximum length is 63 characters.
enable	(Available only in global configuration mode). Enables remote client software updates.
family *family_name*	If the Auto Update client is configured to identify itself by device family, specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.

rev-nums *rev-nums*	(Not available in privileged EXEC mode.) Specifies the software or firmware images for this client. For Windows, WIN9X, WinNT, and vpn3002 clients, enter up to 4, in any order, separated by commas. For security appliances, only one is allowed. The maximum length of the string is 127 characters.
tunnel-group	(Available only in privileged EXEC mode.) Specifies the name of a valid tunnel-group for remote client update.
type *type*	(Not available in privileged EXEC mode.) Specifies the operating systems of remote PCs or the type of security appliances (configured as Auto Update clients) to notify of a client update. The list comprises the following: • asa5505: Cisco 5505 Adaptive Security Appliance • asa5510: Cisco 5510 Adaptive Security Appliance • asa5520: Cisco 5520 Adaptive Security Appliance • asa5540: Cisco Adaptive Security Appliance • linux: A Linux client • mac: MAC OS X client • pix-515: Cisco PIX 515 Firewall • pix-515e: Cisco PIX 515E Firewall • pix-525: Cisco PIX 525 Firewall • pix-535: Cisco PIX 535 Firewall • Windows: all windows-based platforms • WIN9X: Windows 95, Windows 98, and Windows ME platforms • WinNT: Windows NT 4.0, Windows 2000, and Windows XP platforms • vpn3002: VPN 3002 hardware client • A text string of up to 15 characters
url *url-string*	(Not available in privileged EXEC mode.) Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client. The maximum string length is 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added tunnel-group ipsec-attributes configuration mode.
7.2(1)	Added the **component**, **device-id**, and **family** keywords and their arguments to support the security appliance configured as an Auto Update server.

Usage Guidelines

In tunnel-group ipsec-attributes configuration mode, you can apply this attribute only to the IPSec remote-access tunnel-group type.

The **client-update** command lets you enable the update; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 Hardware Client users, the update occurs automatically, with no notification. When the client type is another security appliance, this security appliance acts as an Auto Update server.

To configure the client-update mechanism, do the following steps:

Step 1 In global configuration mode, enable client update by entering the command:

```
hostname(config)# client-update enable
hostname(config)#
```

Step 2 In global configuration mode, configure the parameters for the client update that you want to apply to all clients of a particular type. That is, specify the type of client and the URL or IP address from which to get the updated image. For Auto Update clients, specify the software component—ASDM or boot image. In addition, you must specify a revision number. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client. This command configures the client-update parameters for all clients of the specified type across the entire security appliance. For example:

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

See the Examples section for an illustration of configuring a tunnel group for a VPN 3002 hardware client.

Note For all Windows clients and Auto Update clients, you must use the protocol "http://" or "https://" as the prefix for the URL. For the VPN3002 Hardware Client, you must specify protocol "tftp://" instead.

Alternatively, for Windows clients and VPN3002 Hardware Clients, you can configure client update just for individual tunnel-groups, rather than for all clients of a particular type. (See Step 3.)

Note You can have the browser automatically start an application by including the application name at the end of the URL; for example: **https://support/updates/vpnclient.exe.**

Step 3 After you have enabled client update, you can define a set of client-update parameters for a particular ipsec-ra tunnel group. To do this, in tunnel-group ipsec-attributes mode, specify the tunnel-group name and its type, and the URL or IP address from which to get the updated image. In addition, you must

specify a revision number. If the user's client revision number matches one of the specified revision numbers, there is no need to update the client; for example, to issue a client update for all Windows clients:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

See the Examples section for an illustration of configuring a tunnel group for a VPN 3002 hardware client. VPN 3002 clients update without user intervention, and users receive no notification message.

Step 4 Optionally, you can send a notice to active users with outdated Windows clients that their VPN client needs updating. For these users, a pop-up window appears, offering the opportunity to launch a browser and download the updated software from the site specified in the URL. The only part of this message that you can configure is the URL. (See Step 2 or 3.) Users who are not active get a notification message the next time they log on. You can send this notice to all active clients on all tunnel groups, or you can send it to clients on a particular tunnel group. For example, to notify all active clients on all tunnel groups, you would enter the following command in privileged EXEC mode:

```
hostname# client-update all
hostname#
```

If the user's client revision number matches one of the specified revision numbers, there is no need to update the client, and users receive no notification message. VPN 3002 clients update without user intervention and users receive no notification message.

Note If you specify the client-update type as **windows** (specifying all Windows-based platforms) and later want to enter a client-update type of **win9x** or **winnt** for the same entity, you must first remove the windows client type with the **no** form of the command, then use new client-update commands to specify the new client types.

Examples

The following example, entered in global configuration mode, enables client update for all active remote clients on all tunnel groups:

```
hostname(config)# client-update enable
hostname#
```

The following example applies only to Windows (win9x, winnt, or windows). Entered in global configuration mode, it configures client update parameters for all Windows-based clients. It designates the revision number, 4.7 and the URL for retrieving the update, which is https://support/updates.

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.7
hostname(config)#
```

The following example applies only to VPN 3002 Hardware Clients. Entered in tunnel-group ipsec-attributes configuration mode, it configures client update parameters for the IPSec remote-access tunnel-group "salesgrp". It designates the revision number, 4.7 and uses the TFTP protocol for retrieving the updated software from the site with the IP address 192.168.1.1:

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
```

```
hostname(config-tunnel-ipsec)#
```

The following example shows how to issue a client update for clients that are Cisco 5520 Adaptive Security Appliances configured as Auto Update clients:

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

The following example, entered in privileged EXEC mode, sends a client-update notification to all connected remote clients in the tunnel group named “remotegrp” that need to update their client software. Clients in other groups do not get an update notification:

```
hostname# client-update remotegrp
hostname#
```

Related Commands

Command	Description
clear configure client-update	Clears the entire client-update configuration.
show running-config client-update	Shows the current client-update configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

clock set

To manually set the clock on the security appliance, use the **clock set** command in privileged EXEC mode.

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

Syntax Description

day	Sets the day of the month, from 1 to 31. You can enter the day and month as **april 1** or as **1 april**, for example, depending on your standard date format.
hh:*mm*:*ss*	Sets the hour, minutes, and seconds in 24-hour time. For example, set **20:54:00** for 8:54 pm.
month	Sets the month. Depending on your standard date format, you can enter the day and month as **april 1** or as **1 april**.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you have not entered any **clock** configuration commands, the default time zone for the **clock set** command is UTC. If you change the time zone after you enter the **clock set** command using the **clock timezone** command, the time automatically adjusts to the new time zone. However, if you enter the **clock set** command after you establish the time zone with the **clock timezone** command, then enter the time appropriate for the new time zone and not for UTC. Similarly, if you enter the **clock summer-time** command after the **clock set** command, the time adjusts for daylight saving. If you enter the **clock set** command after the **clock summer-time** command, enter the correct time for daylight saving.

This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other **clock** commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time for the **clock set** command.

Examples

The following example sets the time zone to MST, the daylight saving time to the default period in the U.S., and the current time for MDT to 1:15 p.m. on July 27, 2004:

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

The following example sets the clock to 8:15 on July 27, 2004 in the UTC time zone, and then sets the time zone to MST and the daylight saving time to the default period in the U.S. The end time (1:15 in MDT) is the same as the previous example.

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

Related Commands

Command	Description
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
show clock	Shows the current time.

clock summer-time

To set the date range for daylight saving time for the display of the security appliance time, use the **clock summer-time** command in global configuration mode. To disable the daylight saving time dates, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]]

Syntax Description

date	Specifies the start and end dates for daylight saving time as a specific date in a specific year. If you use this keyword, you need to reset the dates every year.
day	Sets the day of the month, from 1 to 31. You can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
hh:mm	Sets the hour and minutes in 24-hour time.
month	Sets the month as a string. For the **date** command, you can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
offset	(Optional) Sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.
recurring	Specifies the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This keyword lets you set a recurring date range that you do not need to alter yearly. If you do not specify any dates, the security appliance uses the default date range for the United States: from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.
week	(Optional) Specifies the week of the month as an integer between 1 and 4 or as the words **first** or **last**. For example, if the day might fall in the partial fifth week, then specify **last**.
weekday	(Optional) Specifies the day of the week: **Monday**, **Tuesday**, **Wednesday**, and so on.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.
zone	Specifies the time zone as a string, for example, **PDT** for Pacific Daylight Time. When the security appliance shows the daylight saving time according to the date range you set with this command, the time zone changes to the value you set here. See the **clock timezone** to set the base time zone to a zone other than UTC.

Defaults

The default offset is 60 minutes.

The default recurring date range is from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	The default recurring date range was changed to 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Usage Guidelines

For the Southern Hemisphere, the security appliance accepts the start month to be later in the year than the end month, for example, from October to March.

Examples

The following example sets the daylight saving date range for Australia:

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

Some countries start daylight saving on a specific date. In the following example, daylight saving time is configured to start on April 1, 2004, at 3 a.m. and end on October 1, 2004, at 4 a.m.

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show clock	Shows the current time.

clock timezone

To set the time zone for the security appliance clock, use the **clock timezone** command in global configuration mode. To set the time zone back to the default of UTC, use the **no** form of this command. The **clock set** command or the time derived from an NTP server sets the time in UTC. You must set the time zone as an offset of UTC using this command.

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

Syntax Description

zone	Specifies the time zone as a string, for example, **PST** for Pacific Standard Time.
[-]*hours*	Sets the number of hours of offset from UTC. For example, PST is **-8** hours.
minutes	(Optional) Sets the number of minutes of offset from UTC.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To set daylight saving time, see the **clock summer-time** command.

Examples

The following example sets the time zone to Pacific Standard Time, which is -8 hours from UTC:

```
hostname(config)# clock timezone PST -8
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.

Command	Description
ntp server	Identifies an NTP server.
show clock	Shows the current time.

cluster-ctl-file

To use trustpoints that are already created from an existing CTL file stored in Flash memory, use the **cluster-ctl-file** command in CTL file configuration mode. To remove the CTL file configuration so that you can create a new CTL file, use the **no** form of this command.

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

Syntax Description

filename_path	Specifies the path and filename of the CTL file stored on disk or stored in Flash memory.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

When this command is configured, the Phone Proxy parses the CTL file stored in Flash memory and installs the trustpoints from that CTL file and uses that file from Flash in the creation of the new CTL file.

Examples

The following example shows the use of the **cluster-ctl-file** command to parse the CTL file stored in Flash memory to install the trustpoints from that file:

```
hostname(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.

Command	Description
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

cluster encryption

To enable encryption for messages exchanged on the virtual load-balancing cluster, use the **cluster encryption** command in vpn load-balancing configuration mode. To disable encryption, use the **no** form of this command.

cluster encryption

no cluster encryption

Note VPN load balancing requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

This command has no arguments or variables.

Defaults

Encryption is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command turns encryption on or off for messages exchanged on the virtual load-balancing cluster.

Before configuring the **cluster encryption** command, you must have first used the **vpn load-balancing** command to enter VPN load-balancing mode. You must also use the **cluster key** command to configure the cluster shared-secret key before enabling cluster encryption.

Note When using encryption, you must first configure the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If ISAKMP is not enabled on the load-balancing inside interface, you will get an error message when you try to configure cluster encryption.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster encryption** command that enables encryption for the virtual load-balancing cluster:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
cluster key	Specifies the shared-secret key for the cluster.
vpn load-balancing	Enters VPN load-balancing mode.

cluster ip address

To set the IP address of the virtual load-balancing cluster, use the **cluster ip address** command in vpn load-balancing configuration mode. To remove the IP address specification, use the **no** form of this command.

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

Syntax Description

ip-address	The IP address that you want to assign to the virtual load-balancing cluster.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode and configure the interface to which the virtual cluster IP address refers.

The cluster ip address must be on the same subnet as the interface for which you are configuring the virtual cluster.

In the **no** form of the command, if you specify the optional *ip-address* value, it must match the existing cluster IP address before the **no cluster ip address** command can be completed.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster ip address** command that sets the IP address of the virtual load-balancing cluster to 209.165.202.224:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
```

```
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
interface	Sets the interfaces of the device.
nameif	Assigns a name to an interface.
vpn load-balancing	Enters VPN load-balancing mode.

cluster key

To set the shared secret for IPSec site-to-site tunnel exchanges on the virtual load-balancing cluster, use the **cluster key** command in vpn load-balancing configuration mode. To remove this specification, use the **no** form of this command.

cluster key *shared-secret*

no cluster key [*shared-secret*]

Syntax Description

shared-secret	A 3- through 17-character string defining the shared secret for the VPN load-balancing cluster. Special characters can appear in the string, but not spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode. The secret defined in the **cluster key** command is also used for cluster encryption.

You must use the **cluster key** command to configure the shared secret before enabling cluster encryption.

If you specify a value for *shared-secret* in the **no cluster key** form of the command, the shared secret value must match the existing configuration.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster key** command that sets the shared secret of the virtual load-balancing cluster to 123456789:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
```

```
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing mode.

cluster-mode

To specify the security mode of the cluster, use the **cluster-mode** command in phone-proxy configuration mode. To set the security mode of the cluster to the default mode, use the **no** form of this command.

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

Syntax Description

mixed	Specifies the cluster mode to be in mixed mode when configuring the Phone Proxy feature.
nonsecure	Specifies the cluster mode to be in nonsecure mode when configuring the Phone Proxy feature.

Defaults

The default cluster mode is nonsecure.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

When you are configuring the Phone Proxy to run in mixed-mode clusters (both secure and nonsecure modes), you must also configure the LDC issuer in case some phones are configured to be in authenticated or encrypted mode:

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Examples

The following example shows the use of the **cluster-mode** command to set the security mode of the Phone Proxy to mixed (the IP phones will operate in secure and nonsecure modes):

```
hostname(config-phone-proxy)# cluster-mode mixed
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
tls-proxy	Configures the TLS proxy instance.

cluster port

To set the UDP port for the virtual load-balancing cluster, use the **cluster port** command in vpn load-balancing configuration mode. To remove the port specification, use the **no** form of this command.

cluster port *port*

no cluster port [*port*]

Syntax Description

port	The UDP port that you want to assign to the virtual load-balancing cluster.

Defaults

The default cluster port is 9023.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode.

You can specify any valid UDP port number. The range is 1-65535.

If you specify a value for *port* in the **no cluster port** form of the command, the port number specified must match the existing configured port number.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster port address** command that sets the UDP port for the virtual load-balancing cluster to 9023:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
```

```
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters VPN load-balancing mode.

command-alias

To create an alias for a command, use the **command-alias** command in global configuration mode. To remove the alias, use the **no** form of this command. When you enter the command alias, the original command is invoked. You might want to create command aliases to provide shortcuts for long commands, for example.

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

Syntax Description

mode	Specifies the command mode in which you want to create the command alias, for example **exec** (for user and privileged EXEC modes), **configure**, or **interface**.
command_alias	Specifies the new name you want for an existing command.
original_command	Specifies the existing command or command with its keywords for which you want to create the command alias.

Defaults

By default, the following user EXEC mode aliases are configured:

h for **help**

lo for **logout**

p for **ping**

s for **show**

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can create an alias for the first part of any command and still enter the additional keywords and arguments as normal.

When you use CLI help, command aliases are indicated by an asterisk (*), and displayed in the following format:

```
*command-alias=original-command
```

For example, the **lo** command alias displays along with other privileged EXEC mode commands that start with "lo," as follows:

```
hostname# lo?
*lo=logout login  logout
```

You can use the same alias in different modes. For example, you can use "happy" in privileged EXEC mode and configuration mode to alias different commands, as follows:

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

To list only commands and omit aliases, begin your input line with a space. Also, to circumvent command aliases, use a space before entering the command. In the following example, the alias happy is not shown, because there is a space before the happy? command.

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

As with commands, you can use CLI help to display the arguments and keywords that can follow a command alias.

You must enter the complete command alias. Shortened aliases are not accepted. In the following example, the parser does not recognize the command hap as indicating the alias happy:

```
hostname# hap
% Ambiguous command: "hap"
```

Examples

The following example shows how to create a command alias named "**save**" for the **copy running-config startup-config** command:

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

Related Commands

Command	Description
clear configure command-alias	Clears all non-default command aliases.
show running-config command-alias	Displays all non-default command aliases configured.

command-queue

To specify the maximum number of MGCP commands that are queued while waiting for a response, use the **command-queue** command in mgcp-map configuration mode. To remove the configuration, use the **no** form of this command.

command-queue *limit*

no command-queue *limit*

Syntax Description

limit	Specifies the maximum number of commands to queue, from 1 to 2147483647.

Defaults

This command is disabled by default.

The default for the MGCP command queue is 200.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Mgcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **command-queue** command to specify the maximum number of MGCP commands that are queued while waiting for a response. The range of allowed values is from 1 to 4294967295. The default is 200. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

Examples

The following example limits the MGCP command queue to 150 commands:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.

Commands	Description
show mgcp	Displays MGCP configuration and session information.
timeout	Configures the idle timeout after which an MGCP media or MGCP PAT xlate connection will be closed.

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Only the **no** form of this command appears in the configuration.

Examples

The following example shows how to disable RFC 1583-compatible route summary cost calculation:

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

compression

To enable compression for SVC connections and WebVPN connections, use the **compression** command from global configuration mode. To remove the command from the configuration, use the **no** form of the command.

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

Syntax Description

all	Specifies enabling all available compression techniques.
svc	Specifies compression for SVC connections.
http-comp	Specifies compression for WebVPN connections.

Defaults

The default is *all*. All available compression techniques are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

For SVC connections, the **compression** command configured from global configuration mode overrides the **svc compression** command configured in group policy webvpn and username webvpn modes.

For example, if you enter the **svc compression** command for a certain group from group policy webvpn mode, and then you enter **no compression** command from global configuration mode, you override the **svc compression** command settings that you configured for the group.

Conversely, if you turn compression back on with the **compression** command from global configuration mode, any group settings take effect, and those settings ultimately determine the compression behavior.

If you disable compression with the **no compression** command, only new connections are affected. Active connections remain unaffected.

Examples

In the following example, compression is turned on for SVC connections:

```
hostname(config)# compression svc
```

In the next example, compression is disabled for SVC and WebVPN connections:

```
hostname(config)# no compression svc http-comp
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.
svc	Enables or requires the SVC for a specific group or user.
svc compression	Enables compression of http data over an SVC connection for a specific group or user.

config-register

To set the configuration register value that is used the next time you reload the security appliance, use the **config-register** command in global configuration mode. To set the value back to the default, use the **no** form of this command. This command is only supported on the ASA 5500 adaptive security appliance. The configuration register value determines which image to boot from as well as other boot parameters.

config-register *hex_value*

no config-register

Syntax Description

hex_value	Sets the configuration register value as a hexadecimal number from 0x0 to 0xFFFFFFFF. This number represents 32 bits and each hexadecimal character represents 4 bits. Each bit controls a different characteristic. However, bits 32 through 20 are either reserved for future use, cannot be set by the user, or are not currently used by the security appliance; therefore, you can ignore the three characters that represent those bits, because they are always set to 0. The relevent bits are represented by 5 hexadecimal characters: 0x*nnnnn*. You do not need to include preceding 0s. You do need to include trailing 0s. For example, 0x2001 is equivalent to 0x02001; but 0x10000 requires all the zeros. See Table 8-1 for more information about available values for the relevant bits.

Defaults

The default value is 0x1, which boots from the local image and startup configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The five characters are numbered from 0 to 4 from right to left, which is standard for hexadecimal and binary numbers. You can select one value for each character, and mix and match values as appropriate. For example, you can select either 0 or 2 for character number 3. Some values take priority if they conflict with other values. For example, if you set 0x2011, which sets the security appliance to both boot

from the TFTP server and to boot from the local image, the security appliance boots from the TFTP server. Because this value also stipulates that if the TFTP boot fails, the security appliance should boot directly into ROMMON, then the action that specifies to boot from the default image is ignored.

A value of 0 means no action unless otherwise specified.

Table 8-1 lists the actions associated with each hexadecimal character; choose one value for each character:

Table 8-1 Configuration Register Values

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
0x	**0**	**0**	**0**[1]	**0**[2]	**0**[2]
	1 Disables the 10 second ROMMON countdown during startup. Normally, you can press Escape during the countdown to enter ROMMON.	**2** If you set the security appliance to boot from a TFTP server, and the boot fails, then this value boots directly into ROMMON.		**1** Boots from the TFTP server image as specified in the ROMMON Boot Parameters (which is the same as the **boot system tftp** command, if present). This value takes precedence over a value set for character 1.	**1** Boots the image specified by the first **boot system** *local_flash* command. If that image does not load, the security appliance tries to boot each image specified by subsequent **boot system** commands until it boots successfully.
					3, **5**, **7**, **9** Boots the image specified by a particular **boot system** *local_flash* command. Value 3 boots the image specified in the first **boot system** command, value 5 boots the second image, and so on. If the image does not boot successfully, the security appliance does not attempt to fall back to other **boot system** command images (this is the difference between using value 1 and value 3). However, the security appliance has a failsafe feature that in the event of a boot failure attempts to boot from any image found in the root directory of internal Flash memory. If you do not want the failsafe feature to take effect, store your images in a different directory than root.
				4[3] Ignores the startup configuration and loads the default configuration.	**2**, **4**, **6**, **8** From ROMMON, if you enter the **boot** command without any arguments, then the security appliance boots the image specified by a particular **boot system** *local_flash* command. Value 3 boots the image specified in the first **boot system** command, value 5 boots the second image, and so on. This value does not automatically boot an image.
				5 Performs both actions above.	

1. Reserved for future use.
2. If character numbers 0 and 1 are not set to automatically boot an image, then the security appliance boots directly into ROMMON.
3. If you disable password recovery using the **service password-recovery** command, then you cannot set the configuration register to ignore the startup configuration.

The configuration register value is not replicated to a standby unit, but the following warning is displayed when you set the configuration register on the active unit:

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

You can also set the configuration register value in ROMMON using the **confreg** command.

Examples

The following example sets the configuration register to boot from the default image:

```
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
boot	Sets the boot image and startup configuration.
service password-recovery	Enables or disables password recovery.

configure factory-default

To restore the configuration to the factory default, use the **configure factory-default** command in global configuration mode. The factory default configuration is the configuration applied by Cisco to new security appliances. This command is supported on all platforms except for the PIX 525 and PIX 535 security appliances.

configure factory-default [*ip_address* [*mask*]]

Syntax Description

ip_address	Sets the IP address of the management or inside interface, instead of using the default address, 192.168.1.1. See the "Usage Guidelines" sections for more information about which interface is configured for your model.
mask	Sets the subnet mask of the interface. If you do not set a mask, the security appliance uses the mask appropriate for the IP address class.

Defaults

The default IP address and mask are 192.168.1.1 and 255.255.255.0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	A factory default configuration was added for the ASA 5505 adaptive security appliance.

Usage Guidelines

For the PIX 515/515E and the ASA 5510 and higher security appliances, the factory default configuration automatically configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration. For the ASA 5505 adaptive security appliance, the factory default configuration automatically configures interfaces and NAT so that the security appliance is ready to use in your network.

This command is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces, and setting the interface IP address is one of the actions this command takes. This command is also only available in single context mode; a security appliance with a cleared configuration does not have any defined contexts to automatically configure using this command.

This command clears the current running configuration and then configures several commands.

If you set the IP address in the **configure factory-default** command, then the **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal Flash memory using the **write memory** command. The **write memory** command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.

Note This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external Flash memory card. The next time you reload the security appliance after restoring the factory configuration, it boots from the first image in internal Flash memory; if you do not have an image in internal Flash memory, the security appliance does not boot.

To configure additional settings that are useful for a full configuration, see the **setup** command.

ASA 5505 Adaptive Security Appliance Configuration

The default factory configuration for the ASA 5505 adaptive security appliance configures the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address in the **configure factory-default** command, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside using interface PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the security appliance, so a PC connecting to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
```

```
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 and Higher Adaptive Security Appliance Configuration

The default factory configuration for the ASA 5510 and higher adaptive security appliance configures the following:

- The management Management 0/0 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the security appliance, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Security Appliance Configuration

The default factory configuration for the PIX 515/515E security appliance configures the following:

- The inside Ethernet1 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the security appliance, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
```

```
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Examples

The following example resets the configuration to the factory default, assigns the IP address 10.1.1.1 to the interface, and then saves the new configuration as the startup configuration:

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

Related Commands

Command	Description
boot system	Sets the software image from which to boot.
clear configure	Clears the running configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
setup	Prompts you to configure basic settings for the security appliance.
show running-config	Shows the running configuration.

configure http

To merge a configuration file from an HTTP(S) server with the running configuration, use the **configure http** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

configure http[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

Syntax Description

:password	(Optional) For HTTP(S) authentication, specifies the password.
:*port*	(Optional) Specifies the port. For HTTP, the default is 80. For HTTPS, the default is 443.
@	(Optional) If you enter a name and/or a password, precedes the server IP address with an at sign (@).
filename	Specifies the configuration filename.
http[**s**]	Specifies either HTTP or HTTPS.
path	(Optional) Specifies a path to the filename.
server	Specifies the server IP address or name. For IPv6 server addresses, if you specify the port, then you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the port number. For example, enter the following address and port: `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	(Optional) For HTTP(S) authentication, specifies the username.

Defaults

For HTTP, the default port is 80. For HTTPS, the default port is 443.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy http running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure http** command is an alternative for use within a context.

Examples

The following example copies a configuration file from an HTTPS server to the running configuration:

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure memory

To merge the startup configuration with the running configuration, use the **configure memory** command in global configuration mode.

configure memory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the security appliance, and then enter the **configure memory** command to load the new configuration.

This command is equivalent to the **copy startup-config running-config** command.

For multiple context mode, a context startup configuration is at the location specified by the **config-url** command.

Examples

The following example copies the startup configuration to the running configuration:

```
hostname(config)# configure memory
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure net

To merge a configuration file from a TFTP server with the running configuration, use the **configure net** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

configure net [*server***:**[*filename*] | **:***filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the security appliance treats the **tftp-server** command filename as a directory, and adds the **configure net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
*server***:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. For IPv6 server addresses, you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the filename. For example, enter the following address: [fe80::2e0:b6ff:fe01:3b7a] The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy tftp running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure net** command is an alternative for use within a context.

Examples

The following example sets the server and filename in the **tftp-server** command, and then overrides the server using the **configure net** command. The same filename is used.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

The following example overrides the server and the filename. The default path to the filename is /tftpboot/configs/config1. The /tftpboot/ part of the path is included by default when you do not lead the filename with a slash (/). Because you want to override this path, and the file is also in tftpboot, include the tftpboot path in the **configure net** command.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

The following example sets the server only in the **tftp-server** command. The **configure net** command specifies only the filename.

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write net	Copies the running configuration to a TFTP server.

configure terminal

To configure the running configuration at the command line, use the **configure terminal** command in privileged EXEC mode. This command enters global configuration mode, which lets you enter commands that change the configuration.

configure terminal

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example enters global configuration mode:

```
hostname# configure terminal
hostname(config)#
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.

config-url

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode.

config-url *url*

Syntax Description

url	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax: • **disk0:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* For the ASA 5500 series adaptive security appliance, this URL indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This URL indicates the internal Flash memory. • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: – **ap**—ASCII passive mode – **an**—ASCII normal mode – **ip**—(Default) Binary passive mode – **in**—Binary normal mode • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you add a context URL, the system immediately loads the context so that it is running.

Note Enter the **allocate-interface** command(s) before you enter the **config-url** command. The security appliance must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**...). If you enter the **config-url** command first, the security appliance loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

The filename does not require a file extension, although we recommend using ".cfg".

The admin context file must be stored on the internal Flash memory.

If you download a context configuration from an HTTP or HTTPS server, you cannot save changes back to these servers using the **copy running-config startup-config** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

To change the URL, reenter the **config-url** command with a new URL.

The security appliance merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

Examples

The following example sets the admin context to be "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Allocates interfaces to a context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

console timeout

To set the idle timeout for a console connection to the security appliance, use the **console timeout** command in global configuration mode. To disable, use the **no** form of this command.

console timeout *number*

no console timeout [*number*]

Syntax Description

number	Specifies the idle time in minutes (0 through 60) after which the console session ends.

Defaults

The default timeout is 0, which means the console session will not time out.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **console timeout** command sets the timeout value for any authenticated, enable mode, or configuration mode user session to the security appliance. The **console timeout** command does not alter the Telnet or SSH timeouts; these access methods maintain their own timeout values.

The **no console timeout** command resets the console timeout value to the default timeout of 0, which means that the console will not time out.

Examples

The following example shows how to set the console timeout to 15 minutes:

```
hostname(config)# console timeout 15
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

content-length

To restrict HTTP traffic based on the length of the HTTP message body, use the **content-length** command in http-map configuration mode. To remove this command, use the **no** form of this command.

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a message fails this inspection.
allow	Allows the message.
bytes	Specifies the number of bytes. The permitted range is 1 to 65535 for the **min** option and 1 to 50000000 for the **max** option.
drop	Closes the connection.
log	(Optional) Generates a syslog.
max	(Optional) Specifies the maximum content length allowed.
min	Specifies the minimum content length allowed.
reset	Sends a TCP reset message to client and server.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Http-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **content-length** command, the security appliance only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the security appliance to reset the TCP connection and create a syslog entry.

Examples

The following example restricts HTTP traffic to messages 100 bytes or larger and not exceeding 2000 bytes. If a message is outside this range, the security appliance resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

context

To create a security context in the system configuration and enter context configuration mode, use the **context** command in global configuration mode. To remove a context, use the **no** form of this command. In context configuration mode, you can identify the configuration file URL and interfaces that a context can use.

context *name*

no context *name* [**noconfirm**]

Syntax Description

name	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.
noconfirm	(Optional) Removes the context without prompting you for confirmation. This option is useful for automated scripts.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you do not have an admin context (for example, if you clear the configuration) then the first context you add must be the admin context. To add an admin context, see the **admin-context** command. After you specify the admin context, you can enter the **context** command to configure the admin context.

You can only remove a context by editing the system configuration. You cannot remove the current admin context using the **no** form of this command; you can only remove it if you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts and the system execution space.
config-url	Specifies the location of the context configuration.
join-failover-group	Assigns a context to a failover group.
show context	Shows context information.

copy

To copy a file from one location to another, use the **copy** command in privileged EXEC mode.

copy [**/noconfirm** | **/pcap**] {*url* | **running-config** | **startup-config**}
{**running-config** | **startup-config** | *url*}

Syntax Description

/noconfirm	Copies the file without a confirmation prompt.
/pcap	Specifies the defaults of the preconfigured TFTP server. See the **tftp-server** command to configure a default TFTP server.
running-config	Specifies the running configuration stored in memory.

startup-config	Specifies the startup configuration stored in flash memory. The startup configuration for single mode or for the system in multiple context mode is a hidden file in flash memory. From within a context, the location of the startup configuration is specified by the **config-url** command. For example, if you specify an HTTP server for the **config-url** command and then enter the **copy startup-config running-config** command, the security appliance copies the startup configuration from the HTTP server using the admin context interface.
url	Specifies the source or destination file to be copied. Not all combinations of source and destination URLs are allowed. For example, you cannot copy from a remote server to another remote server; this command is meant to copy between local and remote locations. In a context, you can copy the running or startup configuration to a TFTP or FTP server using the context interfaces, but you cannot copy from a server to the running or startup configuration. See the **startup-config** keyword for other options. Also, see the **configure net** command to download from a TFTP server to the running context configuration. See the following URL syntax: • **disk0:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This option indicates the internal flash card. For the ASA 5500 series adaptive security appliance, **flash** is an alias for **disk0**. • **smb:**//[*path*/]*filename* This option indicates the local file system on a UNIX server. • **ftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: – **ap**—ASCII passive mode – **an**—ASCII normal mode – **ip**—(Default) Binary passive mode – **in**—Binary normal mode • **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp://**[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name using the **nameif interface** command if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Added support for DNS names.
8.0(2)	Added the **smb:** URL option

Usage Guidelines

When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

Examples

The following example shows how to copy a file from the disk to a TFTP server in the system execution space:

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

The following example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
hostname(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

The following example shows how to copy an ASDM file from a TFTP server to the internal Flash memory:

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

The following example shows how to copy the running configuration in a context to a TFTP server:

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

The copy command supports DNS names as well as IP addresses as shown in this version of the preceding example:

```
hostname(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

Related Commands

Command	Description
configure net	Copies a file from a TFTP server to the running configuration.
copy capture	Copies a capture file to a TFTP server.
tftp-server	Sets the default TFTP server.

Command	Description
write memory	Saves the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

copy capture

To copy a capture file to a server, use the **copy capture** command in privileged EXEC mode.

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name*/]*buffer_name url*

Syntax Description

/noconfirm	Copies the file without a confirmation prompt.
/pcap	Copies the packet capture as raw data.
buffer_name	Unique name that identifies the capture.
context_name/	Copies a packet capture defined in a security context.
url	Specifies the destination to copy the packet capture file. See the following URL syntax: • **disk0:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the internal Flash card. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the external Flash card. • **flash:**/[*path*/]*filename* This option indicates the internal Flash card. For the ASA 5500 series adaptive security appliance, **flash** is an alias for **disk0**. • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: – **ap**—ASCII passive mode – **an**—ASCII normal mode – **ip**—(Default) Binary passive mode – **in**—Binary normal mode • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	Multiple System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
hostname(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
show capture	Displays the capture configuration when no options are specified.

crashinfo console disable

To read, write, and configure crash write to flash, use the **crashinfo console disable** command in global configuration mode.

crashinfo console disable

no crashinfo console disable

Syntax Description

disable	Suppresses console output in the event of a crash.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	Support for this command was introduced.

Usage Guidelines

This command lets you suppress crashinfo from being output to the console. The crashinfo may contain sensitive information that is not appropriate for viewing by all users connected to the device. In conjunction with this command, you should also ensure crashinfo is written to flash, which can be examined after the device reboots. This command effects output for crashinfo and checkheaps, which is saved to flash and should be sufficient for troubleshooting.

Examples

```
hostname(config)# crashinfo console disable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.

Command	Description
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

crashinfo force

To force the security appliance to crash, use the **crashinfo force** command in privileged EXEC mode.

crashinfo force [**page-fault | watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the security appliance as a result of a page fault.
watchdog	(Optional) Forces a crash of the security appliance as a result of watchdogging.

Defaults

The security appliance saves the crash information file to flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The security appliance reloads after the crash dump is complete.

Caution Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the security appliance and forces it to reload.

Examples

The following example shows the warning that displays when you enter the **crashinfo force page-fault** command:

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

If you enter a carriage return (by pressing the Return or Enter key on your keyboard), "**Y**", or "**y**" the security appliance crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a **no**, and the security appliance returns to the command-line prompt.

Related Commands

clear crashinfo	Clears the contents of the crash information file.
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash information file.

crashinfo save disable

To disable crash information from writing to Flash memory, use the **crashinfo save** command in global configuration mode. To allow the crash information to be written to Flash memory, and return to the default behavior, use the **no** form of this command.

crashinfo save disable

no crashinfo save disable

Syntax Description

This command has no default arguments or keywords.

Defaults

The security appliance saves the crash information file to Flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	The **crashinfo save enable** command was deprecated and is no longer a valid option. Use the **no crashinfo save disable** command instead.

Usage Guidelines

Crash information writes to Flash memory first, and then to your console.

Note If the security appliance crashes during startup, the crash information file is not saved. The security appliance must be fully initialized and running first, before it can save crash information to Flash memory.

Use the **no crashinfo save disable** command to re-enable saving the crash information to Flash memory.

Examples

```
hostname(config)# crashinfo save disable
```

Related Commands

clear crashinfo	Clears the contents of the crash file.
crashinfo force	Forces a crash of the security appliance.

crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file.

crashinfo test

To test the ability of the security appliance to save crash information to a file in flash memory, use the **crashinfo test** command in privileged EXEC mode.

crashinfo test

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If a previous crash information file already exists in flash memory, that file is overwritten.

Note Entering the **crashinfo test** command does not crash the security appliance.

Examples

The following example shows the output of a crash information file test.

```
hostname# crashinfo test
```

Related Commands

clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces the security appliance to crash.
crashinfo save disable	Disables crash information from writing to Flash memory.
show crashinfo	Displays the contents of the crash file.

crl

To specify CRL configuration options, use the **crl** command in crypto ca trustpoint configuration mode.

crl {**required | optional | nocheck**}

Syntax Description

required	The required CRL must be available for a peer certificate to be validated.
optional	The security appliance can still accept the peer certificate if the required CRL is not available.
nocheck	Directs the security appliance not to perform CRL checking.

Defaults

The default value is **nocheck**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command was deprecated. The following permutations of the **revocation-check** command replace it. • **revocation-check crl none** replaces **crl optional** • **revocation-check crl** replaces **crl required** • **revocation-check none** replaces **crl nocheck**

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and requires that a CRL be available for a peer certificate to be validated for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint submode.
crl configure	Enters crl configuration mode.

crl configure

To enter CRL configuration mode, use the **crl configure** command in crypto ca trustpoint configuration mode.

crl configure

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters crl configuration mode within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint configuration mode.

CHAPTER 9

crypto ca authenticate through customization Commands

crypto ca authenticate

To install and authenticate the CA certificates associated with a trustpoint, use the **crypto ca authenticate** command in global configuration mode. To remove the CA certificate, use the **no** form of this command.

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

no crypto ca authenticate *trustpoint*

Syntax Description

fingerprint	Specifies a hash value consisting of alphanumeric characters the security appliance uses to authenticate the CA certificate. If a fingerprint is provided, the security appliance compares it to the computed fingerprint of the CA certificate and accepts the certificate only if the two values match. If there is no fingerprint, the security appliance displays the computed fingerprint and asks whether to accept the certificate.
hexvalue	Identifies he hexadecimal value of the fingerprint.
nointeractive	Obtains the CA certificate for this trustpoint using no interactive mode; intended for use by the device manager only. In this case, if there is no fingerprint, the security appliance accepts the certificate without question.
trustpoint	Specifies the trustpoint from which to obtain the CA certificate. Maximum name length is 128 characters.

Defaults

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced

Usage Guidelines

If the trustpoint is configured for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, the security appliance prompts you to paste the base-64 formatted CA certificate onto the terminal.

The invocations of this command do not become part of the running configuration.

Examples

The following example shows the security appliance requesting the certificate of the CA. The CA sends its certificate and the security appliance prompts the administrator to verify the certificate of the CA by checking the CA certificate fingerprint. The security appliance administrator should verify the fingerprint value displayed against a known, correct value. If the fingerprint displayed by the security appliance matches the correct value, you should accept the certificate as valid.

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

In the next example, the trustpoint tp9 is configured for terminal-based (manual) enrollment. In this case thesecurity appliance prompts the administrator to paste the CA certificate to the terminal. After displaying the fingerprint of the certificate, the security appliance prompts the administrator to confirm that the certificate should be retained.

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

Related Commands

Command	Description
crypto ca enroll	Starts enrollment with a CA.
crypto ca import certificate	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca certificate chain

To enter certificate chain configuration mode for the indicated trustpoint, use the **crypto ca certificate chain** command in global configuration mode. To return to global configuration mode, use the **exit** command.

crypto ca certificate chain *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint for configuring the certificate chain.

Defaults

This command has no default values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters CA certificate chain submode for trustpoint central:

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.

crypto ca certificate map

To enter CA certificate map mode, use the **crypto ca configuration map** command in global configuration mode. Executing this command places you in ca-certificate-map mode. Use this group of commands to maintain a prioritized list of certificate mapping rules. The sequence number orders the mapping rules. To remove a crypto CA configuration map rule, use the **no** form of the command.

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

Syntax Description

map-name	Specifies a name for a certificate-to-group map.
sequence-number	Specifies a number for the certificate map rule you are creating. The range is 1 through 65535. You can use this number when creating a tunnel-group-map, which maps a tunnel group to a certificate map rule.

Defaults

No default behavior or values for sequence-number.

The default value for *map-name* is DefaultCertificateMap.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.
7.2	Added keyword *map-name*.

Usage Guidelines

Issuing this command places the security appliance in CA certificate map configuration mode where the user can configure rules based on the certificate's issuer and subject distinguished names (DNs). The general form of these rules is as follows:

DN match-criteria match-value

DN is either *subject-name* or *issuer-name*. DNs are defined in the ITU-T X.509 standard. For a list of certificate fields, see Related Commands.

match-criteria comprise the following expressions or operators:

attr *tag*	Limits the comparison to a specific DN attribute, such as common name (CN).
co	Contains
eq	Equal
nc	Does not contain
ne	Not equal

The DN matching expressions are case insensitive.

Examples

The following example enters CA certificate map mode with a map named example-map and a sequence number of 1 (rule # 1), and specifies that the common name(CN) attribute of the subject-name must match Example1:

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name attr cn eq Example1
hostname(ca-certificate-map)#
```

The following example enters CA certificate map mode with a map named example-map and a sequence number of 1, and specifies that the subject-name contain the value cisco anywhere within it:

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

Related Commands

Command	Description
issuer-name	Indicates that rule entry is applied to the issuer DN of the IPSec peer certificate.
subject-name (crypto ca certificate map)	Indicates that rule entry is applied to the subject DN of the IPSec peer certificate.
tunnel-group-map enable	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

crypto ca crl request

To request a CRL based on the configuration parameters of the specified trustpoint, use the **crypto ca crl request** command in crypto ca trustpoint configuration mode.

crypto ca crl request *trustpoint*

Syntax Description

trustpoint	Specifies the trustpoint. Maximum number of characters is 128.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the running configuration.

Examples

The following example requests a CRL based on the trustpoint named central:

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.

crypto ca enroll

To start the enrollment process with the CA, use the **crypto ca enroll** command in global configuration mode. For this command to execute successfully, the trustpoint must have been configured correctly.

crypto ca enroll *trustpoint* [**noconfirm**]

Syntax Description

noconfirm	(Optional) Suppresses all prompts. Enrollment options that might have been prompted for must be pre-configured in the trustpoint. This option is for use in scripts, ASDM, or other such non-interactive needs.
trustpoint	Specifies the name of the trustpoint to enroll with. Maximum number of characters is 128.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When the trustpoint is configured for SCEP enrollment, the security appliance displays a CLI prompt immediately and displays status messages to the console asynchronously. When the trustpoint is configured for manual enrollment, the security appliance writes a base-64-encoded PKCS10 certification request to the console and then displays the CLI prompt.

This command generates interactive prompts that vary depending on the configured state of the referenced trustpoint.

Examples

The following example enrolls for an identity certificate with trustpoint tp1 using SCEP enrollment. The security appliance prompts for information not stored in the trustpoint configuration.

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
```

```
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

The next command shows manual enrollment of a CA certificate.

```
hostname(config)# crypto ca enroll tp1
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca import pkcs12	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca export

To export the security appliance trustpoint configuration with all associated keys and certificates in PKCS12 format, or to export the device's identity certificate in PEM format, use the **crypto ca export** command in global configuration mode.

crypto ca export *trustpoint* **identify-certificate**

Syntax Description

identify-certificate	Specifies that the enrolled certificate associated with the named trustpoint is to be displayed on the console.
trustpoint	Specifies the name of the trustpoint whose certificate is to be displayed. Maximum number of characters for a trustpoint name is 128.

Defaults

This command has no default values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.
8.0(2)	This command was changed to accommodate certificate exporting in PEM format.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The PEM or PKCS12 data is written to the console.

Web browsers use the PKCS12 format to store private keys with accompanying public key certificates protected with a password-based symmetric key. The security device exports the certificates and keys associated with a trust point in base64-encoded PKCS12 format. This feature can be used to move certificates and keys between security devices.

PEM encoding of a certificate is a base64 encoding of an X.509 certificate enclosed by PEM headers. This provides a standard method for text-based transfer of certificates between security devices. PEM encoding can be used to export the *proxy-ldc-issuer* certificate utilizing SSL/TLS protocol proxy when the security device is acting as a client.

Examples

The following example exports the PEM-formatted certificate for trustpoint 222 as a console display:

```
hostname (config)# crypto ca export 222 identity-certificate
```

```
Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
hostname (config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.
crypto ca trustpoint	Enters the trustpoint configuration mode for the indicated trustpoint.

crypto ca import

To install a certificate received from a CA in response to a manual enrollment request or to import the certificate and key pair for a trustpoint using PKCS12 data, use the **crypto ca import** command in global configuration mode. The security appliance prompts you to paste the text to the terminal in base 64 format.

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

Syntax Description

trustpoint	Specifies the trustpoint with which to associate the import action. Maximum number of characters is 128. If you import PKCS12 data and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint.
certificate	Tells the security appliance to import a certificate from the CA represented by the trustpoint.
pkcs12	Tells the security appliance to import a certificate and key pair for a trustpoint, using PKCS12 format.
passphrase	Specifies the passphrase used to decrypt the PKCS12 data.
nointeractive	(Optional) Imports a certificate using nointeractive mode. This suppresses all prompts. This option for use in scripts, ASDM, or other such non-interactive needs.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example manually imports a certificate for the trustpoint Main:

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
```

```
quit
INFO: Certificate successfully imported
hostname (config)#
```

The following example manually imports PKCS12 data to trustpoint central:

```
hostname (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

Related Commands

Command	Description
crypto ca export	Exports a trustpoint certificate and key pair in PKCS12 format.
crypto ca authenticate	Obtains the CA certificate for a trustpoint.
crypto ca enroll	Starts enrollment with a CA.
crypto ca trustpoint	Enters the trustpoint submode for the indicated trustpoint.

crypto ca server

To set up and manage a local CA server on the security appliance, use the **crypto ca server** command in global configuration mode to enter config-ca-server configuration mode and access the CA configuration commands. To delete the configured local CA server from the security appliance, use the **no** form of this command.

crypto ca server

no crypto ca server

Defaults

A certificate authority server is not enabled on the security appliance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

There can only be one local CA on a security appliance.

The **crypto ca server** command configures the CA server but does not enable it. Use the **no** version of the **shutdown** command in config-ca-server mode to enable the local CA.

When you activate the CA server with the **no shutdown** command, you establish the RSA keypair of the CA and a trustpoint named LOCAL-CA-SERVER to hold the self-signed certificate. This newly-generated self-signed certificate always has ‘digital signature’, ‘crl signing’ and ‘certificate signing’ key usage settings set.

Caution The **no crypto ca server** command deletes the configured local CA server, its RSA keypair and associated trustpoint, regardless of the local CA server’s current state.

Examples

The following example uses the command to enter config-ca-server configuration mode and then uses the question-mark to list the local CA server commands available in that mode:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
```

```
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

The following example uses the **no** form of the **crypto ca server** command in config-ca-server mode to delete the configured and enabled CA server from the security appliance:

```
hostname(config-ca-server)#no crypto ca server

Certificate server 'remove server' event has been queued for processing.
hostname(config)#
```

Related Commands

Command	Description
debug crypto ca server	Shows debug messages when you configure the local CA server.
show crypto ca server	Displays the status and parameters of the configured CA server.
show crypto ca server cert-db	Displays local CA server certificates.

crypto ca server crl issue

To force the issuance of a Certificate Revocation List (CRL), use the **crypto ca server crl issue** command in privileged EXEC mode.

crypto ca server crl issue

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This seldom-used command is employed to recover a lost CRL. Normally, the CRL is reissued automatically upon expiration by resigning the existing CRL. The **crypto ca server crl issue** command regenerates the CRL based on the certificate database and should only be used as required to regenerate a CRL based on the certificate database contents.

Examples

The following example forces the issuance of a CRL by the local CA server:

```
hostname(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point to be include in the certificates issued by the CA.
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows the user to configure and manage the local CA.

Command	Description
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
show crypto ca server crl	Displays the current CRL of the local CA.

crypto ca server revoke

To mark a certificate issued by the local Certificate Authority (CA) server as revoked in the certificate database and the CRL, use the **crypto ca server revoke** command in privileged EXEC mode.

crypto ca server revoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of certificate to be revoked. Enter the serial number in hexadecimal format.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You revoke a specific certificate that has been issued by the local CA on a security appliance by entering the **crypto ca server revoke** command on that security appliance. Revocation is accomplished when this command marks the certificate as revoked in the certificate database on the CA server and in the CRL. You specify the certificate to be revoked by entering the certificate serial number in hex format.

The CRL is regenerated automatically after the specified certificate is revoked.

Examples

The following example revokes the certificate with the serial number 782ea09f issued by the local CA server:

```
hostname(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server unrevoke	Unrevokes a previously revoked certificate issued by the local CA server.
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server crl	Displays the current CRL of the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server unrevoke

To unrevoke a previously revoked certificate issued by the local CA server, use the **crypto ca server unrevoke** command in privileged EXEC mode.

crypto ca server unrevoke *cert-serial-no*

Syntax Description

cert-serial-no	Specifies the serial number of certificate to be unrevoked. Enter the serial number in hexadecimal format.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You unrevoke a previously revoked certificate issued by the local CA on a security appliance by entering the **crypto ca server unrevoke** command. The validity of the certificate is restored when this command marks the certificate as valid in the certificate database and removes it from the CRL. You specify the certificate to be unrevoked by entering the certificate serial number in hexadecimal format.

The CRL is regenerated automatically after the specified certificate is unrevoked.

Examples

The following example unrevokes the certificate with the serial number 782ea09f issued by the local CA server:

```
hostname(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been
issued.
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
crypto ca server user-db add	Adds a user to the CA server user database.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db add

To insert a new user into the CA server user database, use the **crypto ca server user-db add** command in privileged EXEC mode.

crypto ca server user-db add *user* [**dn** *dn*] **[email** *e-mail-address*]

Syntax Description

dn *dn*	Specifies a subject-name distinguished name for certificates issued to the added user. If a DN string contains a comma, enclose the value string with double quotes (for example, O="Company, Inc.")
email *e-mail-address*	Specifies the e-mail address for the new user.
user	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or an e-mail address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The *user* argument can be a simple username such as jandoe or an e-mail address such as jandoe@example.com. The *username* must match the username specified by the end user in the enrollment page.

The *username* is added to the database as a user without privileges. You must use the **crypto ca server allow** command to grant enrollment privileges.

username, along with the one-time password, is used to enroll the user on the enrollment interface page.

Note For e-mail notification of the one-time password (OTP), an e-mail address should be specified either in the *username* or *email-address* field. A missing e-mail address at mailing time generates an error.

The *user* argument, **email**, is used only as an e-mail address to notify the user for enrollment and renewal reminders and does not appear in the issued certificate.

Inclusion of the e-mail address ensures that the user can be contacted with any questions and is notified of the required one-time password for enrollment.

If a optional *dn* is not specified for a user, the subject name dn is formed using the *username* and the subject-name-default DN setting as cn=*username*,subject-name-default.

Examples

The following example adds a user to the user database with a username of jandoe@example.com along with a complete subject-name DN:

```
hostname(config-ca-server)# crypto ca server user-db add dn "cn=Jan Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
hostname(config-ca-server)#
```

The following example grants enrollment privileges to the user named jondoe.

```
hostname(config-ca-server)# crypto ca server user-db allow jondoe
hostname(config-ca-server)
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
crypto ca server user-db allow	Permits a specific user or a subset of users in the CA server database to enroll with the CA.
crypto ca server user-db remove	Deletes a user from the CA server database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
database path	Specifies a path or location for the local CA database. The default location is flash memory.

crypto ca server user-db allow

To permit a user or a group of users to enroll in the local CA server database, use the **crypto ca server user-db allow** command in privileged EXEC mode. This command also includes options to generate and display one-time passwords or to e-mail them to the users.

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]

Syntax Description

all-certholders	Specifies that enrollment privileges be granted to all users in the database who have been issued a certificate, whether the certificate is currently valid or not. This is equivalent to granting renewal privileges.
all-unenrolled	Specifies that enrollment privileges be granted to all users in the database who have not been issued a certificate.
email-otp	(Optional) Sends the specified users one-time passwords by e-mail to their configured e-mail addresses.
replace-otp	(Optional) Specifies that one-time passwords be regenerated for all specified users who originally had valid one-time passwords.
display-otp	(Optional) Displays the one-time passwords for all specified users to the console.
username	Specifies a single user to whom to grant enrollment privileges. The username can be a simple username or e-mail address.

Defaults

No default behavior or values.

.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **replace-otp** keyword generates OTPs for all specified users. These new OTPs replace any valid ones previously generated for the specified users.

Note that the OTP is not stored on the security device but is generated and regenerated as required to notify a user or to authenticate a user during enrollment.

Examples

The following example grants enrollment privileges to all users in the database who have not enrolled yet:

```
hostname(config-ca-server)# crypto ca server user-db allow all-unenrolled
hostname(config-ca-server)#
```

The following example grants enrollment privileges to the user named user1:

```
hostname(config-ca-server)# crypto ca server user-db allow user1
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db write	Copies the user information in the CA server database to the file specified by the **database path** command.
enrollment-retrieval	Specifies the time in hours that an enrolled user can retrieve a PKCS12 enrollment file.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db email-otp

To e-mail the OTP to a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db email-otp** command in privileged EXEC mode.

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

Syntax Description

all-certholders	Specifies that OTPs is e-mailed to all users in the database who have been issued a certificate, whether that certificate is currently valid or not.
all-unenrolled	Specifies that the OTPs is e-mailed to all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user is e-mailed to that user. The username can be a simple username or e-mail address.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example e-mails the OTP to all unenrolled users in the database:

```
hostname(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
hostname(config-ca-server)#
```

The following example e-mails the OTP to the user named user1:

```
hostname(config-ca-server)# crypto ca server user-db email-otp user1
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server user-db show-otp	Displays the one-time password for a specific user or a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca server user-db remove

To remove a user from the local CA server user database, use the **crypto ca server user-db remove** command in privileged EXEC mode.

crypto ca server user-db remove *username*

Syntax Description

username	Specifies the name of the user to remove in the form of a username or an e-mail address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command removes a username from the CA user database so that user cannot enroll. The command also provideees the option to revoke previously issued, valid certificates.

Examples

The following example removes a user with a username, user1, from the CA server user database :

```
hostname(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.

Command	Description
show crypto ca server user-db	Displays users included in the CA server user database.
crypto ca server user-db write	Writes the user information configured in the local CA database to the file specified by the **database path** command.

crypto ca server user-db show-otp

To display the OTP for a specific user or a subset of users in the local CA server database, use the **crypto ca server user-db show-otp** command in privileged EXEC mode.

crypto ca server user-db show-otp {*username* | **all-certholders** | **all-unenrolled**}

Syntax Description

all-certholders	Displays the OTPs for all users in the database who have been issued a certificate, whether the certificate is currently valid or not.
all-unenrolled	Displays the OTPs for all users in the database who have never been issued a certificate, or who only hold expired or revoked certificate(s).
username	Specifies that the OTP for a single user be displayed. The username can be a simple username or e-mail address.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example displays the OTP for all users who have valid or invalid certificates in the database:

```
hostname(config-ca-server)# crypto ca server user-db show-otp all-certholders
hostname(config-ca-server)#
```

The following example displays the OTP for the user named user1:

```
hostname(config-ca-server)# crypto ca server user-db show-otp user1
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db allow	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
crypto ca server user-db email-otp	E-mails the one-time password to a specific user or to a subset of users in the CA server database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

crypto ca server user-db write

To configure a directory location to store all the local CA database files, use the **crypto ca server user-db write** command in privileged EXEC mode.

crypto ca server user-db write

Syntax Description

This command has no keywords or arguments.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **crypto ca server user-db write** command is used to save new user-based configuration data to the storage specifed by the database path configuration. The information is generated when new users are added or allowed with the **crypto ca server user-db add** and **crypto ca server user-db allow** commands.

Examples

The following example writes the user information configured in the local CA database to storage:

```
hostname(config-ca-server)# crypto ca server user-db write
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
database path	Specifies a path or location for the local CA database. The default location is flash memory.

Command	Description
crypto ca server user-db remove	Removes a user from the CA server user database.
show crypto ca server cert-db	Displays all certificates issued by the local CA.
show crypto ca server user-db	Displays users included in the CA server user database.

crypto ca trustpoint

To enter the trustpoint configuration mode for the specified trustpoint, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command.

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm]**

Syntax Description

noconfirm	Suppresses all interactive prompting
trustpoint- name	Identifies the name of the trustpoint to manage. The maximum name length is 128 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Subcommands added to support Online Certificate Status Protocol. These include **match certificate map**, **ocsp disable-nonce**, **ocsp url**, and **revocation-check**.
8.0(2)	Subcommands added to support certificate validation. These include **id-usage** and **validation-policy.** The following are being deprecated: **accept-subordinates, id-cert-issuer**, and **support-user-cert-validation**.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA. Issuing this command puts you in crypto ca trustpoint configuration mode.

This command manages trustpoint information. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub mode control CA-specific configuration parameters which specify how the security appliance obtains the CA certificate, how the security appliance obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

You can specify characteristics for the trustpoint using the following commands listed alphabetically in this command reference guide:

- **accept-subordinates**— Indicates whether CA certificates subordinate to the CA associated with the trustpoint are accepted if delivered during phase one IKE exchange when not previously installed on the device.
- **client-types**—Specifies the client connection types for which this trustpoint can be sued to validate the certificates associated with a user connection.
- **crl required | optional | nocheck**—Specifies CRL configuration options.
- **crl configure**—Enters CRL configuration mode (see **crl**).
- **default enrollment**—Returns all enrollment parameters to their system default values. Invocations of this command do not become part of the active configuration.
- **email** *address*—During enrollment, asks the CA to include the specified email address in the Subject Alternative Name extension of the certificate.
- **enrollment retry period** —Specifies a retry period in minutes for SCEP enrollment.
- **enrollment retry count**—Specifies a maximum number of permitted retries for SCEP enrollment.
- **enrollment terminal**—Specifies cut and paste enrollment with this trustpoint.
- **enrollment url** *url*—Specifies SCEP enrollment to enroll with this trustpoint and configures the enrollment URL (*url*).
- **exit**—Leaves the configuration mode.
- **fqdn** *fqdn*—During enrollment, asks the CA to include the specified FQDN in the Subject Alternative Name extension of the certificate.
- **id-cert-issuer**—Deprecated. Indicates whether the system accepts peer certificates issued by the CA associated with this trustpoint.
- **id-usage**— Specifies how the enrolled identity of a trustpoint can be used.
- **ignore-ipsec-keyusage**—Deprecated. Suppress key usage checking on IPsec client certificates.
- **ignore-ssl-keyusage**—Deprecated. Suppress key usage checking on SSL client certificates.
- **ip-addr** *ip-address*—During enrollment, asks the CA to include the IP address of the security appliance in the certificate.
- **keypair** *name*—Specifies the key pair whose public key is to be certified.
- **match certificate** *map-name* **override ocsp**—Matches a certificate map to an OCSP override rule.
- **ocsp disable-nonce**—Disables the nonce extension, which cryptographically binds revocation requests with responses to avoid replay attacks.
- **ocsp url**—Specifies that the OCSP server at this URL checks all certificates associated with this trustpoint for revocation status.
- **password** *string*—Specifies a challenge phrase that is registered with the CA during enrollment. The CA typically uses this phrase to authenticate a subsequent revocation request.
- **proxy-ldc-issuer**—An issuer for TLS proxy local dynamic certificates.
- **revocation check**—Specifies the revocation checking method, which include CRL, OCSP, and none.
- **serial-number**—During enrollment, asks the CA to include the security appliance's serial number in the certificate.
- **subject-name** *X.500 name*—During enrollment, asks the CA to include the specified subject DN in the certificate.

- **support-user-cert-validation**—Deprecated. If enabled, the configuration settings to validate a remote user certificate can be taken from this trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate. This option applies to the configuration data associated with the subcommands **crl required | optional | nocheck** and all settings in the CRL sub mode.
- **validation-policy**—Deprecated. Specifies trustpoint conditions for validating certificates associated with user connections.

Examples

The following example enters CA trustpoint mode for managing a trustpoint named central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca authenticate	Obtains the CA certificate for this trustpoint.
crypto ca certificate map	Enters crypto CA certificate map mode. Defines certificate-based ACLs.
crypto ca crl request	Requests a CRL based on configuration parameters of specified trustpoint.
crypto ca import	Installs a certificate received from a CA in response to a manual enrollment request. Also used to import PKS12 data to a trustpoint.

crypto dynamic-map match address

To match address of anaccess list for the dynamic crypto map entry, use the **crypto dynamic-map match address** command in global configuration mode. To disable the address match, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

Syntax Description

acl-name	Identifies the access-list to be matched for the dynamic crypto map entry.
dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

See the **crypto map match address** command for additional information about this command.

Examples

The following example shows the use of the **crypto dynamic-map** command to match address of an access list named aclist1:

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto dynamic-map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto may entry, use the **no** form of this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

Syntax Description

dynamic-map-name	Specifies the name of the crypto dynamic map set.
dynamic-seq-num	Specifies the number you assign to the crypto dynamic map entry.

Defaults

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto dynamic-map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command disables NAT-T for the crypto dynamic map named mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set peer

See the **crypto map set peer** command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
ip_address	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the **name** command.
hostname	Identifies the peer in the dynamic crypto map entry by hostname, as defined by the **name** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address10.0.0.1:

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set pfs

To specify the dynamic crypto map sets, use the **crypto map dynamic-map set pfs** command in global configuration mode. To remove the specified dynamic-map crypto map set, use the **no** form of this command.

See the **crypto map set pfs** command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5]**

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
group1	Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPSec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
set pfs	Configures IPSec to ask for perfect forward secrecy (PFS) when requesting new security associations for this dynamic crypto map entry or configures IPSec to require PFS when receiving requests for new security associations.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was modified to add Diffie-Hellman group 7.
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

The **crypto dynamic-map** commands, such as **match address**, **set peer**, and **set pfs** are described with the **crypto map** commands. If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the security appliance assumes a default of group2. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

When interacting with the Cisco VPN Client, the security appliance does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto dynamic-map mymap 10. The group specified is group 2:

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set reverse route

See the **crypto map set reverse-route** command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

Syntax Description

dynamic-map-name	Specifies the name of the crypto map set.
dynamic-seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default value for this command is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following command enables RRI for the crypto dynamic-map named mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all configuration for all the dynamic crypto maps.
show running-config crypto dynamic-map	Displays all configuration for all the dynamic crypto maps.

crypto dynamic-map set transform-set

To specify the transform sets to use in a dynamic crypto map entry, use the **crypto dynamic-map set transform-set** command in global configuration mode.

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

Specify the names of the transform sets in the **no** form of this command to remove them from a dynamic crypto map entry.

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

Using the **no** form of the command while specifying all or none of the transform sets removes the dynamic crypto map entry.

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set**

Syntax Description

dynamic-map-name	Specifies the name of the dynamic crypto map set.
dynamic-seq-num	Specifies the sequence number that corresponds to the dynamic crypto map entry.
transform-set-name1 *transform-set-name11*	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec transform-set** command. Each crypto map entry supports up to 11 transform sets.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	Changed maximum number of transform sets in a crypto map entry.

Usage Guidelines

A dynamic crypto map is a crypto map without all of the parameters configured. It acts as a policy template where the missing parameters are later dynamically learned, as the result of an IPSec negotiation, to match the peer requirements. The security appliance applies a dynamic crypto map to let a peer negotiate a tunnel if its IP address is not already identified in a static crypto map. This occurs with the following types of peers:

- Peers with dynamically assigned public IP addresses.

  Both LAN-to-LAN and remote access peers can use DHCP to obtain a public IP address. The security appliance uses this address only to initiate the tunnel.

- Peers with dynamically assigned private IP addresses.

  Peers requesting remote access tunnels typically have private IP addresses assigned by the headend. Generally, LAN-to-LAN tunnels have a predetermined set of private networks that are used to configure static maps and therefore used to establish IPSec SAs.

As an administrator configuring static crypto maps, you might not know the IP addresses that are dynamically assigned (via DHCP or some other method), and you might not know the private IP addresses of other clients, regardless of how they were assigned. VPN clients typically do not have static IP addresses; they require a dynamic crypto map to allow IPSec negotiation to occur. For example, the headend assigns the IP address to a Cisco VPN client during IKE negotiation, which the client then uses to negotiate IPSec SAs.

Dynamic crypto maps can ease IPSec configuration and we recommend them for use in networks where the peers are not always predetermined. Use dynamic crypto maps for Cisco VPN clients (such as mobile users) and routers that obtain dynamically assigned IP addresses.

Tip Use care when using the **any** keyword in **permit** entries in dynamic crypto maps. If the traffic covered by such a **permit** entry could include multicast or broadcast traffic, insert **deny** entries for the appropriate address range into the access list. Remember to insert **deny** entries for network and subnet broadcast traffic, and for any other traffic that IPSec should not protect.

Dynamic crypto maps work only to negotiate SAs with remote peers that initiate the connection. The security appliance cannot use dynamic crypto maps to initiate connections to a remote peer. With a dynamic crypto map configured, if the outbound traffic matches a permit entry in an access list and the corresponding SA does not yet exist, the security appliance drops the traffic.

A crypto map set may include a dynamic crypto map. Dynamic crypto map sets should be the lowest priority crypto maps in the crypto map set (that is, they should have the highest sequence numbers) so that the security appliance evaluates other crypto maps first. It examines the dynamic crypto map set only when the other (static) map entries do not match.

Similar to static crypto map sets, a dynamic crypto map set consists of all of the dynamic crypto maps with the same dynamic-map-name. The dynamic-seq-num differentiates the dynamic crypto maps in a set. If you configure a dynamic crypto map, insert a permit ACL to identify the data flow of the IPSec peer for the crypto access list. Otherwise the security appliance accepts any data flow identity the peer proposes.

Caution Do not assign static (default) routes for traffic to be tunneled to a security appliance interface configured with a dynamic crypto map set. To identify the traffic that should be tunneled, add the ACLs to the dynamic crypto map. Use care to identify the proper address pools when configuring the ACLs associated with remote access tunnels. Use Reverse Route Injection to install routes only after the tunnel is up.

You can combine static and dynamic map entries within a single crypto map set.

Examples

The following example creates a dynamic crypto map entry named “dynamic0” consisting of the same ten transform sets. The “crypto ipsec transform-set (create or remove transform set)” section shows ten transform set example commands.

```
hostname(config)# crypto dynamic-map dynamic0 1 set transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec transform-set	Configures a transform set.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto ipsec df-bit

To configure DF-bit policy for IPSec packets, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

Syntax Description

clear-df	(Optional) Specifies that the outer IP header will have the DF bit cleared and that the security appliance may fragment the packet to add the IPSec encapsulation.
copy-df	(Optional) Specifies that the security appliance will look in the original packet for the outer DF bit setting.
set-df	(Optional) Specifies that the outer IP header will have the DF bit set; however, the security appliance may fragment the packet if the original packet had the DF bit cleared.
interface	Specifies an interface name.

Defaults

This command is disabled by default. If this command is enabled without a specified setting, the security appliance uses the **copy-df** setting as default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The DF bit with IPSec tunnels feature lets you specify whether the security appliance can clear, set, or copy the Don't Fragment (DF) bit from the encapsulated header. The DF bit within the IP header determines whether a device is allowed to fragment a packet.

Use the **crypto ipsec df-bit** command in global configuration mode to configure the security appliance to specify the DF bit in an encapsulated header.

When encapsulating tunnel mode IPSec traffic, use the **clear-df** setting for the DF bit. This setting lets the device send packets larger than the available MTU size. Also this setting is appropriate if you do not know the available MTU size.

Examples

The following example, entered in global configuration mode, sets the IPSec DF policy to **clear-df**:

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.
show crypto ipsec fragmentation	Displays the fragmentation policy for a specified interface.

crypto ipsec fragmentation

To configure the fragmentation policy for IPSec packets, use the **crypto ipsec fragmentation** command in global configuration mode.

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

Syntax Description

after-encryption	Specifies the security appliance to fragment IPSec packets that are close to the maximum MTU size after encryption (disables pre-fragmentation).
before-encryption	Specifies the security appliance to fragment IPSec packets that are close to the maximum MTU size before encryption (enables pre-fragmentation).
interface	Specifies an interface name.

Defaults

This feature is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting security appliance, and it is encapsulated with IPSec headers, it is likely to exceed the MTU of the outbound link. This causes packet fragmentation after encryption, which makes the decrypting device reassemble in the process path. Pre-fragmentation for IPSec VPNs increases the performance of the device when decrypting by letting it operate in the high performance CEF path instead of the process path.

Pre-fragmentation for IPSec VPNs lets an encrypting device predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec SA. If the device predetermines that the packet will exceed the MTU of the output interface, the device fragments the packet before encrypting it. This avoids process level reassembly before decryption and helps improve decryption performance and overall IPsec traffic throughput.

Examples

The following example, entered in global configuration mode, enables pre-fragmentation for IPSec packets globally on the device:

```
hostname(config)# crypto ipsec fragmentation before-encryption inside
hostname(config)#
```

The following example, entered in global configuration mode, disables pre-fragmentation for IPSec packets on the interface:

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the DF-bit policy for IPSec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

crypto ipsec security-association lifetime

To configure global lifetime values, use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset a crypto ipsec entry lifetime value to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

Syntax Description

kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes.The default is 4,608,000 kilobytes.
seconds	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The default is 28,800 seconds (eight hours).
token	Indicates a token-based server for user authentication is used.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **crypto ipsec security-association lifetime** command changes global lifetime values used when negotiating IPSec security associations.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has no lifetime values configured, when the security appliance requests new security associations during negotiation, it specifies its global lifetime value in the request to the peer; it uses this value as the lifetime of the new security associations. When the security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached.

The security appliance lets the user change crypto map, dynamic map, and ipsec settings on the fly. If this is changed, the security appliance brings down only the connections affected by the change. If the user changes an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes require more CPU processing time for establishing new security associations.

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed or after the amount of traffic in kilobytes has passed.

Examples

The following example specifies a global timed lifetime for security associations:

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPSec configuration (i.e. global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec security-association replay

To configure the IPSec anti-replay window size, use the **crypto ipsec security-association replay** command in global configuration mode. To reset the window size to the default value, use the **no** form of this command.

crypto ipsec security-association replay {**window-size** *n* | **disable**}

no crypto ipsec security-association replay {**window-size** *n* | **disable**}

Syntax Description

n	Sets the window size. Values can be 64, 128, 256, 512, or 1024. The default is 64.
disable	Disables anti-replay checking.

Defaults

The default window size is 64.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

Cisco IPsec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, QoS gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor; this event can generate warning syslog messages that are false alarms. The **crypto ipsec security-association replay** command lets you expand the window size, allowing the decryptor to keep track of more than 64 packets.

Increasing the anti-replay window size has no impact on throughput and security. The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed to store the sequence number on the decryptor. It is recommended that you use the full 1024 window size to eliminate any future anti-replay problems.

Examples

The following example specifies the anti-replay window size for security associations:

```
hostname(config)# crypto ipsec security-association replay window-size 1024
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all IPSec configuration (i.e. global lifetimes and transform sets).
shape	Enables traffic shaping.
priority	Enables priority queueing.
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec transform-set (create or remove transform set)

To create or remove a transform set, use the **crypto ipsec transform-set** command in global configuration mode. With **crypto ipsec transform-set** command, the user can identify the IPSec encryption and hash algorithms to be used by the transform set. Tto remove a transform set, use the **no** form of this command.

crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

no crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

Syntax Description

authentication	(Optional) Specify one of the following authentication methods to ensure the integrity of IPSec data flows: **esp-md5-hmac** to use the MD5/HMAC-128 as the hash algorithm. **esp-sha-hmac** to use the SHA/HMAC-160 as the hash algorithm. **esp-none** to not use HMAC authentication.
encryption	Specify one of the following encryption methods to protect IPSec data flows: **esp-aes** to use AES with a 128-bit key. **esp-aes-192** to use AES with a 192-bit key. **esp-aes-256** to use AES with a 256-bit key. **esp-des** to use 56-bit DES-CBC. **esp-3des** to use triple DES algorithm. **esp-null** to not use encryption.
transform-set-name	Name of the transform-set being created or modified. To view the transform sets already present in the configuration, enter the **show running-config ipsec** command.

Defaults

The default authentication setting is esp-none (no authentication).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	This section was rewritten.

Usage Guidelines

Following the configuration of a transform set, you assign it to a crypto map. You can assign up to six transform sets to a crypto map. When the peer attempts to establish an IPSec session, the security appliance evaluates the peer against the access list of each crypto map until it finds a match. The security appliance then evaluates all of the protocols, algorithms, and other settings negotiated by the peer against those in the transform sets assigned to the crypto map until it finds a match. If the security appliance matches the peer's IPSec negotiations to the settings in a transform set, it applies them to the protected traffic as part of its IPSec security association. The security appliance terminates the IPSec session if it fails to match the peer to an access list and find an exact match of the security settings of the peer to those in a transform set assigned to the crypto map.

You can specify either the encryption or the authentication first. You can specify the encryption without specifying the authentication. If you specify the authentication in a transform set you are creating, you must specify the encryption with it. If you specify only the authentication in a transform set you are modifying, the transform set retains its current encryption setting.

If you are using AES encryption, we recommend that you use the **isakmp policy priority group 5** command, also in in global configuration mode, to assign Diffie-Hellman group 5 to accommodate the large key sizes provided by AES.

Tip When you apply transform sets to a crypto map or a dynamic crypto map and view the transform sets assigned to it, you will find it helpful if the names of the transform sets reflect their configuration. For example, the name "3des-md5" in the first example below shows the encryption and authentication used in the transform set. The values that follow the name are the actual encryption and authentication settings assigned to the transform set.

Examples

The following commands show all possible encryption and authentication options, excluding those that specify no encryption and no authentication:

```
hostname(config)# crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 56des-md5 esp-des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 56des-sha esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 128aes-md5 esp-aes esp-md5-hmac
hostname(config)# crypto ipsec transform-set 128aes-sha esp-aes esp-sha-hmac
hostname(config)# crypto ipsec transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 192aes-sha esp-aes-192 esp-sha-hmac
hostname(config)# crypto ipsec transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 256aes-sha esp-aes-256 esp-sha-hmac
hostname(config)#
```

Related Commands

Command	Description
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

crypto isakmp am-disable

To disable inbound aggressive mode connections, use the **crypto isakmp am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

crypto isakmp am-disable

no crypto isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp am-disable** command was introduced.
7.2.(1)	The **crypto isakmp am-disable** command replaces the **isakmp am-disable** command**.**

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
hostname(config)# crypto isakmp am-disable
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp disconnect-notify

To enable disconnect notification to peers, use the **crypto isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp disconnect-notify** command was introduced.
7.2.(1)	The **crypto isakmp disconnect-notify** command replaces the **isakmp disconnect-notify** command**.**

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# crypto isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance, use the **crypto isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

crypto isakmp enable *interface-name*

no crypto isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This **isakmp enable** command was preexisting.
7.2(1)	The **crypto isakmp enable** command replaces the **isakmp enable** command.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
hostname(config)# no crypto isakmp enable inside
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp identity

To set the Phase 2 ID to be sent to the peer, use the **crypto isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISAKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully-qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Defaults

The default ISAKMP identity is **crypto isakmp identity auto**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	The **isakmp identity** command was preexisting.
7.2(1)	The **crypto isakmp identity** command replaces the **isakmp identity** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPSec peer, depending on connection type:

```
hostname(config)# crypto isakmp identity auto
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp ipsec-over-tcp

To enable IPSec over TCP, use the **crypto isakmp ipsec-over-tcp** command in global configuration mode. To disable IPSec over TCP, use the **no** form of this command.

crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

no crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPSec over TCP connections. You can list up to 10 ports. Port numbers can be in the range 1-65535. The default port number is 10000.

Defaults

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp ipsec-over-tcp** command was introduced.
7.2.(1)	The **crypto isakmp ipsec-over-tcp** command replaces the **isakmp ipsec-over-tcp** command**.**

Examples

This example, entered in global configuration mode, enables IPSec over TCP on port 45:

```
hostname(config)# crypto isakmp ipsec-over-tcp port 45
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you enable it with the **crypto isakmp enable** command) in global configuration mode. To disable the NAT traversal, use the **no** form of this command.

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Defaults

By default, NAT traversal is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp nat-traversal** command was preexisting.
7.2.(1)	The **crypto isakmp nat-traversal** command replaces the **isakmp nat-traversal** command**.**
8.0(2)	NAT traversal is now enabled by default.

Usage Guidelines

NAT including PAT is used in many networks where IPSec is also used, but there are a number of incompatibilities that prevent IPSec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The security appliance supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html, and supports NAT traversal for both dynamic and static crypto maps.

This command enables NAT-T globally on the security appliance. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then sets NAT traversal with a keepalive interval of 30 seconds:

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy authentication

To specify an authentication method within an IKE policy, use the **crypto isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To remove the ISAKMP authentication method, use the related **clear configure** command.

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

Syntax Description

crack	Specifies IKE CRACK as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This basically means you can prove to a third party whether you had an IKE negotiation with the peer.

Defaults

The default ISAKMP policy authentication is **pre-share**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy authentication** command was preexisting.
7.2.(1)	The **crypto isakmp policy authentication** command replaces the **isakmp policy authentication** command**.**

Usage Guidelines

If you specify RSA signatures, you must configure the security appliance and its peer to obtain certificates from a CA server. If you specify preshared keys, you must separately configure these preshared keys within the security appliance and its peer.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy authentication** command. This example sets the authentication method of RSA Signatures to be used for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **crypto isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is **des,** use the **no** form of this command.

crypto isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no crypto isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

Syntax Description

3des	Specifies that the Triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default ISAKMP policy encryption is **3des**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy encryption** command was preexisting.
7.2.(1)	The **crypto isakmp policy encryption** command replaces the **isakmp policy encryption** command**.**

Examples

The following example, entered in global configuration mode, shows use of the **crypto isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
hostname(config)# crypto isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 encryption 3des
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **crypto isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default group policy is group 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy group** command was introduced.
7.2(1)	The **crypto isakmp policy group** command replaces the **isakmp policy group** command**.**
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires isakmp policy to use DH group 2. (If you configure DH group 1, the Cisco VPN Client cannot connect.)

AES support is available on security appliances licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) group 5 instead of group 1 or group 2. To configures group 5, use the **crypto isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy group** command. This example sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 group 2
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **crypto isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

crypto isakmp policy *priority* **hash** {**md5 | sha**}

no crypto isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm for the IKE policy.
priority	Uniquely identifies and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies SHA-1 (HMAC variant) as the hash algorithm for the IKE policy.

Defaults

The default hash algorithm is SHA-1 (HMAC variant).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy hash** command was preexisting.
7.2.(1)	The **crypto isakmp policy hash** command replaces the **isakmp policy hash** command**.**

Usage Guidelines

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, shows how to use the **crypto isakmp policy hash** command. This example specifies the MD5 hash algorithm for the IKE policy, with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 hash md5
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **crypto isakmp policy lifetime** command in global configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for infinite lifetime.

Defaults

The default value is 86,400 seconds (one day).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp policy lifetime** command was preexisting.
7.2.(1)	The **crypto isakmp policy lifetime** command replaces the **isakmp policy lifetime** command**.**

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPSec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the security appliance sets up future IPSec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) for the IKE policy with the priority number of 40.

```
hostname(config)# crypto isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
hostname(config)# crypto isakmp policy 40 lifetime 0
```

Related Commands

clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the security appliance, use the **crypto isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the security appliance, use the **no** form of this command.

crypto isakmp reload-wait

no crypto isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **isakmp reload-wait** command was introduced.
7.2.(1)	The **crypto isakmp reload-wait** command replaces the **isakmp reload-wait** command**.**

Examples

The following example, entered in global configuration mode, tells the security appliance to wait until all active sessions have terminated before rebooting.

```
hostname(config)# crypto isakmp reload-wait
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
show running-config crypto isakmp	Displays all the active configuration.

crypto key generate dsa

To generate DSA key pairs for identity certificates, use the **crypto key generate dsa** command in global configuration mode.

crypto key generate dsa {**label** *key-pair-label*} [**modulus** *size*] [**noconfirm**]

Syntax Description

label *key-pair-label*	Specifies the name to be associated with the key pair(s); maximum label length is 128 characters. DSA requires a label.
modulus *size*	Specifies the modulus size of the key pair(s): 512, 768, 1024. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.

Defaults

The default modulus size is 1024.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **crypto key generate dsa** command to generate DSA key pairs to support SSL, SSH, and IPSec connections. The generated key pairs are identified by labels that you provide as part of the command syntax. If you do not provide a label, the security appliance displays an error message.

Note When generating DSA keys, you may encounter a delay. On a Cisco PIX 515E Firewall, this delay may extend up to few minutes.

Examples

The following example, entered in global configuration mode, generates an DSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate dsa label mypubkey
INFO: The name for the keys will be: mypubkey
hostname(config)#
```

The following example, entered in global configuration mode, inadvertently attempts to generate a duplicate DSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate dsa label mypubkey
```

```
WARNING: You already have dSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new DSA keys named mypubkey
hostname(config)#
```

Related Commands

Command	Description
crypto key zeroize	Removes the DSA key pairs.
show crypto key mypubkey	Displays the DSA key pairs.

crypto key generate rsa

To generate RSA key pairs for identity certificates, use the **crypto key generate rsa** command in global configuration mode.

crypto key generate rsa [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

Syntax Description

general-keys	Generates a single pair of general purpose keys. This is the default key-pair type.
label *key-pair-label*	Specifies the name to be associated with the key pair(s). This key pair must be uniquely labeled. If you attempt to create another key pair with the same label, the security appliance displays an warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>.
modulus *size*	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
noconfirm	Suppresses all interactive prompting.
usage-keys	Generates two key pairs, one for signature use and one for encryption use. This implies that two certificates for the corresponding identity are required.

Defaults

The default key-pair type is **general key**. The default modulus size is 1024.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **crypto key generate rsa** command to generate RSA key pairs to support SSL, SSH, and IPSec connections. The generated key pairs are identified by labels that you can provide as part of the command syntax. Trustpoints that do not reference a key pair can use the default one <Default-RSA-Key>. SSH connections always use this key. This does not affect SSL, since SSL generates its own cert/key dynamically, unless a trustpoint has one configured.

Caution Many SSL connections using identity certificates with RSA key pairs that exceed 1024 bits can cause a high CPU usage on the security appliance and rejected clientless logins.

Examples

The following example, entered in global configuration mode, generates an RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

The following example, entered in global configuration mode, inadvertently attempts to generate a duplicate RSA key pair with the label mypubkey:

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

The following example, entered in global configuration mode, generates an RSA key pair with the default label:

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

Related Commands

Command	Description
crypto key zeroize	Removes RSA key pairs.
show crypto key mypubkey	Displays the RSA key pairs.

crypto key zeroize

To remove the key pairs of the indicated type (rsa or dsa), use the **crypto key zeroize** command in global configuration mode.

crypto key zeroize {**rsa | dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

Syntax Description

default	Removes RSA key pairs with no labels. This keyword is legal only with RSA key pairs.
dsa	Specifies DSA as the key type.
label *key-pair-label*	Removes the key pairs of the indicated type (rsa or dsa). If you do not provide a label, the security appliance removes all key pairs of the indicated type.
noconfirm	Suppresses all interactive prompting.
rsa	Specifies RSA as the key type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, removes all RSA key pairs:

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

Related Commands

Command	Description
crypto key generate dsa	Generates DSA key pairs for identity certificates.
crypto key generate rsa	Generate RSA key pairs for identity certificates.

crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command in global configuration mode. To remove the crypto map set from the interface, use the **no** form of this command.

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

Syntax Description

interface-name	Specifies the interface for the security appliance to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a CA to obtain certificates, this should be the interface with the address specified in the CA certificates.
map-name	Specifies the name of the crypto map set.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use this command to assign a crypto map set to any active security appliance interface. The security appliance supports IPSec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPSec services.

You can assign only one crypto map set to an interface. If multiple crypto map entries have the same *map-name* but a different *seq-num*, they are part of the same set and are all applied to the interface. The security appliance evaluates the crypto map entry with the lowest *seq-num* first.

Note The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

Every static crypto map must define three parts: an access list, a transform set, and an IPsec peer. If one of these is missing, the crypto map is incomplete and the security appliance moves on to the next entry. However, if the crypto map matches on the access-list but not on either or both of the other two requirements, this security appliance drops the traffic.

Use the **show running-config crypto map** command to ensure that every crypto map is complete. To fix an incomplete crypto map, remove the crypto map, add the missing entries, and reapply it.

Examples

The following example, entered in global configuration mode, assigns the crypto map set named mymap to the outside interface. When traffic passes through the outside interface, the security appliance evaluates it against all the crypto map entries in the mymap set. When outbound traffic matches an access list in one of the mymap crypto map entries, the security appliance forms a security association using that crypto map entry's configuration.

```
hostname(config)# crypto map mymap interface outside
```

The following example shows the minimum required crypto map configuration:

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map ipsec-isakmp dynamic

To require a given crypto map entry to refer to a pre-existing dynamic crypto map, use the **crypto map ipsec-isakmp dynamic** command in global configuration mode. Use the **no** form of this command to remove the cross reference.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Syntax Description

dynamic-map-name	Specifies the name of the crypto map entry that refers to a pre-existing dynamic crypto map.
ipsec-isakmp	Indicates that IKE establishes the IPSec security associations for this crypto map entry.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was modified to remove the **ipsec-manual** keyword.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the dynamic crypto map set to interfaces.

Dynamic crypto maps provide two functions: filtering/classifying traffic to protect, and defining the policy to apply to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec dynamic crypto maps identify the following:

- The traffic to protect
- IPSec peer(s) with which to establish a security association
- Transform sets to use with the protected traffic

- How to use or manage keys and security associations

A crypto map set is a collection of crypto map entries, each with a different sequence number (seq-num) but the same map name. Therefore, for a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPSec security applied. To accomplish this you create two crypto map entries, each with the same map name, but each with a different sequence number.

The number you assign as the seq-num argument should not be arbitrary. This number ranks multiple crypto map entries within a crypto map set. A crypto map entry with a lower seq-num is evaluated before a map entry with a higher seq-num; that is, the map entry with the lower number has a higher priority.

Note When you link the crypto map to a dynamic crypto map, you must specify the dynamic crypto map. This links the crypto map to an existing dynamic crypto map that was previously defined using the **crypto dynamic-map** command. Now any changes you make to the crypto map entry after it has been converted, will not take affect. For example, a change to the set peer setting does not take effect. However, the security appliance stores the change while it is up. When the dynamic crypto map is converted back to the crypto map, the change is effective and appears in the output of the **show running-config crypto map** command. The security appliance maintains these settings until it reboots.

Examples

The following command, entered in global configuration mode, configures the crypto map mymap to refer to a dynamic crypto map named test.

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map match address

To assign an access list to a crypto map entry, use the **crypto map match address** command in global configuration mode. To remove the access list from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

Syntax Description

acl_name	Specifies the name of the encryption access list. This name should match the name argument of the named encryption access list being matched.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list** command to define the access lists.

The security appliance uses the access lists to differentiate the traffic to protect with IPSec crypto from the traffic that does not need protection. It protects outbound packets that match a permit ACE, and ensures that inbound packets that match a permit ACE have protections.

When the security appliance matches a packet to a deny statement, it skips the evaluation of the packet against the remaining ACEs in the crypto map, and resumes evaluation of the packet against the ACEs in the next crypto map in sequence. *Cascading ACLs* involves the use of deny ACEs to bypass evaluation of the remaining ACEs in an ACL, and the resumption of evaluation of traffic against the ACL assigned to the next crypto map in the crypto map set. Because you can associate each crypto map with different IPSec settings, you can use deny ACEs to exclude special traffic from further evaluation in the corresponding crypto map, and match the special traffic to permit statements in another crypto map to provide or require different security.

Note The crypto access list does not determine whether to permit or deny traffic through the interface. An access list applied directly to the interface with the **access-group** command makes that determination.

In transparent mode, the destination address should be the IP address of the security appliance, the management address. Only tunnels to the security appliance are allowed in transparent mode.

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set connection-type

To specify the connection type for the Backup Site-to-Site feature for this crypto map entry, use the **crypto map set connection-type** command in global configuration mode. Use the **no** form of this command to return to the default setting.

crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

no crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

Syntax Description

answer-only	Specifies that this peer only responds to inbound IKE connections first during the initial proprietary exchange to determine the appropriate peer to connect to.
bidirectional	Specifies that this peer can accept and originate connections based on this crypto map entry. This is the default connection type for all Site-to-Site connections.
map-*name*	Specifies the name of the crypto map set.
originate-only	Specifies that this peer initiates the first proprietary exchange to determine the appropriate peer to connect to.
seq-num	Specifies the number you assign to the crypto map entry.
set connection-type	Specifies the connection type for the Backup Site-to-Site feature for this crypto map entry. There are three types of connections: answer-only, originate-only, and bidirectional.

Defaults

The default setting is bidirectional.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **crypto map set connection-type** command specifies the connection types for the Backup Lan-to-Lan feature. It allows multiple backup peers to be specified at one end of the connection.

This feature works only between the following platforms:

- Two Cisco ASA 5500 series security appliances

- A Cisco ASA 5500 series security appliance and a Cisco VPN 3000 concentrator
- A Cisco ASA 5500 series security appliance and a security appliance running Cisco PIX security appliance software v7.0, or higher

To configure a backup Lan-to-Lan connection, we recommend you configure one end of the connection as originate-only using the **originate-only** keyword, and the end with multiple backup peers as answer-only using the **answer-only** keyword. On the originate-only end, use the **crypto map set peer** command to order the priority of the peers. The originate-only security appliance attempts to negotiate with the first peer in the list. If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list.

When configured in this way, the originate-only peer initially attempts to establish a proprietary tunnel and negotiate with a peer. Thereafter, either peer can establish a normal Lan-to-Lan connection and data from either end can initiate the tunnel connection.

In transparent firewall mode, you can see this command but the connection-type value cannot be set to anything other than answer-only for crypto map entries that are part of a crypto map that has been attached to the interface.

Table 9-1 lists all supported configurations. Other combinations may result in unpredictable routing issues.

Table 9-1 Supported Backup LAN-to-LAN Connection Types

Remote Side	Central Side
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the connection-type to originate-only.

```
hostname(config)# crypto map mymap 10 set connection-type originate-only
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set inheritance

To set the granularity (single or multiple) of security associations generated for this crypto map entry, use the **set inheritance** command in global configuration mode. To remove the inheritance setting for this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set inheritance {data| rule}**

no crypto map *map-name seq-num* **set inheritance {data | rule}**

Syntax Description

data	Specifies one tunnel for every address pair within the address ranges specified in the rule.
map-name	Specifies the name of the crypto map set.
rule	Specifies one tunnel for each ACL entry associated with this crypto map. Default.
seq-num	Specifies the number you assign to the crypto map entry.
set inheritance	Specifies the type of inheritance: **data or rule**. Inheritance allows a single security association (SA) to be generated for each security policy database (SPD) rule or multiple security SAs for each address pair in the range.

Defaults

Default value is **rule**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command works only when the security appliance is initiating the tunnel, not when responding to a tunnel. Using the data setting may create a large number of IPSec SAs. This consumes memory and results in fewer overall tunnels. You should use the data setting only for extremely security-sensitive applications.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the inheritance type to data.

```
hostname(config)# crypto map mymap 10 set inheritance data
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set nat-t-disable

To disable NAT-T for connections based on this crypto map entry, use the **crypto map set nat-t-disable** command in global configuration mode. To enable NAT-T for this crypto may entry, use the **no** form of this command.

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default setting for this command is not on (therefore NAT-T is enabled by default).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **isakmp nat-traversal** command to globally enable NAT-T. Then you can use the **crypto map set nat-t-disable** command to disable NAT-T for specific crypto map entries.

Examples

The following command, entered in global configuration mode, disables NAT-T for the crypto map entry named mymap.

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
isakmp nat-traversal	Enables NAT-T for all connections.
show running-config crypto map	Displays the crypto map configuration.

crypto map set peer

To specify an IPSec peer in a crypto map entry, use the **crypto map set peer** command in global configuration mode. Use the **no** form of this command to remove an IPSec peer from a crypto map entry.

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

Syntax Description

hostname	Specifies a peer by its host name as defined by the security appliance **name** command.
ip_address	Specifies a peer by its IP address.
map-name	Specifies the name of the crypto map set.
peer	Specifies an IPSec peer in a crypto map entry either by hostname of IP address.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was modified to allow up to 10 peer addresses.

Usage Guidelines

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used because, in general, the peer is unknown.

Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the security appliance attempts to negotiate with the first peer in the list. If that peer does not respond, the security appliance works its way down the list until either a peer responds or there are no more peers in the list. You can set up multiple peers only when using the backup LAN-to-LAN feature (that is, when the crypto map connection type is originate-only). For more information, see the **crypto map set connection-type** command.

Examples

The following example, entered in global configuration mode, shows a crypto map configuration using IKE to establish the security associations. In this example, you can set up a security association to either the peer at 10.0.0.1 or the peer at 10.0.0.2.

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set pfs

Use the **crypto map set pfs** command in global configuration mode to set IPSec to ask for PFS when requesting new security associations for this crypto map entry or that IPSec requires PFS when receiving requests for new security associations. To specify that IPSec should not request PFS, use the **no** form of this command.

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5]**

Syntax Description

group1	Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPSec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

By default PFS is not set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was modified to add Diffie-Hellman group 7.
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

With PFS, every time a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security because if one key is ever cracked by an attacker, only the data sent with that key is compromised.

During negotiation, this command causes IPSec to request PFS when requesting new security associations for the crypto map entry. If the **set pfs** statement does not specify a group, the security appliance sends the default (group2).

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, the security appliance assumes a default of group2. If the local configuration specifies group2, or group5, that group must be part of the peer's offer or the negotiation fails.

For a negotiation to succed PFS has to be set on both ends. If set, the groups have to be an exact match; The security appliance does not accept just any offer of PFS from the peer.

The 1536-bit Diffie-Hellman prime modulus group, group5, provides more security than group1, or group2, but requires more processing time than the other groups.

When interacting with the Cisco VPN Client, the security appliance does not use the PFS value, but instead uses the value negotiated during Phase 1.

Examples

The following example, entered in global configuration mode, specifies that PFS should be used whenever a new security association is negotiated for the crypto map "mymap 10":

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

Related Commands

Command	Description
clear isakmp sa	Deletes the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel-groups and their parameters.

crypto map set phase1-mode

To specify the IKE mode for phase 1 when initiating a connection to either main or aggressive, use the **crypto map set phase1 mode** command in global configuration mode. To remove the setting for phase 1 IKE negotiations, use the **no** form of this command. Including a Diffie-Hellman group with aggressive mode is optional. If one is not included, the security appliance uses group 2.

crypto map *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

no crypto map *map-name seq-num* **set phase1-mode {main | aggressive [group1 | group2 | group5]}**

Syntax Description

aggressive	Specifies aggressive mode for phase one IKE negotiations
group1	Specifies that IPSec should use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group2	Specifies that IPSec should use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
group5	Specifies that IPSec should use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
main	Specifies main mode for phase one IKE negotiations.
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

Default phase one mode is **main**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

This command works only in initiator mode; not in responder mode.

Examples

The following example, entered in global configuration mode, configures the crypto map my map and sets the phase one mode to aggressive, using group 2.

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

Related Commands

Command	Description
clear isakmp sa	Delete the active IKE security associations.
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set reverse-route

To enable RRI for any connection based on this crypto map entry, use the **crypto map set reverse-route** command in global configuration mode. To disable reverse route injection for any connection based this crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set reverse-route**

no crypto map *map-name seq-num s***et reverse-route**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default setting for this command is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The security appliance can automatically add static routes to the routing table and announce these routes to its private network or border routers using OSPF.

Examples

The following example, entered in global configuration mode, enables RRI for the crypto map named mymap.

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations, use the **crypto map set security-association lifetime** command in global configuration mode. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

Syntax Description

kilobytes	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The default is 4,608,000 kilobytes.
map-name	Specifies the name of the crypto map set.
seconds	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default number of kilobytes is 4,608,000; the default number of seconds is 28,800.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the security appliance requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the security appliance receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The session keys/security association expires after the first of these lifetimes is reached. You can specify both with one command.

Note The security appliance lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the security appliance brings down only the connections affected by the change. If you change an existing access-list associated with a crypto map, specifically by deleting an entry within the access-list, the result is that only the associated connection is brought down. Connections based on other entries in the access-list are not affected.

To change the timed lifetime, use the **crypto map set security-association lifetime seconds** command. The timed lifetime causes the keys and security association to time out after the specified number of seconds have passed.

Examples

The following command, entered in global configuration mode, specifies a security association lifetime in seconds and kilobytes for crypto map mymap:

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.

crypto map set transform-set

To specify the transform sets to use in a crypto map entry, use the **crypto map set transform-set** command in global configuration mode.

crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

To specifically remove the names of the transform sets from a crypto map entry, use the **no** form of this commandwith the specified transform set name.

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

To specify all or none of the transform sets and remove the crypto map entry, use the **no** form of the command.

no crypto map *map-name seq-num* **set transform-set**

Syntax Description

map-name	Specifies the name of the crypto map set.
seq-num	Specifies the sequence number that corresponds to the crypto map entry.
transform-set-name1 *transform-set-name11*	Specifies one or more names of the transform sets. Any transform sets named in this command must be defined in the **crypto ipsec transform-set** command. Each crypto map entry supports up to 11 transform sets.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	Changed maximum number of transform sets in a crypto map entry.

Usage Guidelines

This command is required for all crypto map entries.

The peer at the opposite end of the IPSec initiation uses the first matching transform set for the security association. If the local security appliance initiates the negotiation, the order specified in the **crypto map** command determines the order in which thesecurity appliance presents the contents of the transform sets to the peer. If the peer initiates the negotiation, the local security appliance uses the first transform set in the crypto map entry that matches the IPSec parameters sent by the peer.

If the peer at the opposite end of the IPSec initiation fails to match the values of the transform sets, IPSec does not establish a security association. The initiator drops the traffic because there is no security association to protect it.

To change the list of transform sets, respecify the new list to replace the old one.

If you use this command to modify a crypto map, the security appliance modifies only the crypto map entry with the same sequence number you specify. For example, the security appliance inserts the transform set named "56des-sha" in the last position if you enter the following commands:

```
hostname(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
hostname(config)# crypto map map1 1 transform-set 56des-sha
hostname(config)#
```

The response to the following command shows the cumulative effect of the previous two commands:

```
hostname(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

To reconfigure the sequence of transform sets in a crypto map entry, delete the entry, specifying both the map name and sequence number; then recreate it. For example, the following commands reconfigure the crypto map entry named map2, sequence 3:

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

Examples

The "crypto ipsec transform-set (create or remove transform set)" section shows ten transform set example commands. The following example creates a crypto map entry named "map2" consisting of the same ten transform sets.

```
hostname(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

The following example, entered in global configuration mode, shows the minimum required crypto map configuration when the security appliance uses IKE to establish the security associations:

```
hostname(config)# crypto map map2 10 ipsec-isakmp
hostname(config)# crypto map map2 10 match address 101
hostname(config)# crypto map map2 set transform-set 3des-md5
hostname(config)# crypto map map2 set peer 10.0.0.1
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto dynamic-map	Clears all dynamic crypto maps from the configuration.
clear configure crypto map	Clears all crypto maps from the configuration.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
crypto ipsec transform-set	Configures a transform set.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.
show running-config crypto map	Displays the crypto map configuration.

crypto map set trustpoint

To specify the trustpoint that identifies the certificate to send for authentication during Phase 1 negotiations for the crypto map entry, use the **crypto map set trustpoint** command in global configuration mode. To remove a trustpoint from a crypto map entry, use the **no** form of this command.

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

Syntax Description

chain	(Optional) Sends a certificate chain. A CA certificate chain includes all CA certificates in a hierarchy of certificates from the root certificate to the identity certificate. The default value is disable (no chain).
map-name	Specifies the name of the crypto map set.
seq-num	Specifies the number you assign to the crypto map entry.
trustpoint-name	Identifies the certificate to be sent during Phase 1 negotiations. The default is none.
token	Indicate a token-based server for user authentication is used.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This crypto map command is valid only for initiating a connection. For information on the responder side, see the **tunnel-group** commands.

Examples

The following example, entered in global configuration mode, specifies a trustpoint named tpoint1 for crypto map mymap and includes the chain of certificates.

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
tunnel-group	Configures tunnel groups.

csc

To enable the adaptive security appliance to send network traffic to the CSC SSM, use the **csc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

csc {**fail-open** | **fail-close**}

no csc

Syntax Description

fail-close	Specifies that the adaptive security appliance should block traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.
fail-open	Specifies that the adaptive security appliance should allow traffic if the CSC SSM fails. This applies to the traffic selected by the class map only. Other traffic not sent to the CSC SSM is not affected by a CSC SSM failure.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **csc** command configures a security policy to send to the CSC SSM all traffic that is matched by the applicable class map. This occurs before the adaptive security appliance allows the traffic to continue to its destination.

You can specify how the security appliance treats matching traffic when the CSC SSM is not available to scan the traffic. The **fail-open** keyword specifies that the security appliance permits the traffic to continue to its destination even though the CSC SSM is not available. The **fail-close** keyword specifies that the security appliance never lets matching traffic continue to its destination when the CSC SSM is not available.

The CSC SSM can scan HTTP, SMTP, POP3, and FTP traffic. It supports these protocols only when the destination port of the packet requesting the connection is the well-known port for the protocol, that is, CSC SSM can scan only the following connections:

- FTP connections opened to TCP port 21.

- HTTP connections opened to TCP port 80.
- POP3 connections opened to TCP port 110.
- SMTP connections opened to TCP port 25.

If policies using the **csc** command select connections that misuse these ports for other protocols, the security appliance passes the packets to the CSC SSM; however, the CSC SSM passes the packets without scanning them.

To maximize the efficiency of the CSC SSM, configure class maps used by policies implementing the **csc** command as follows:

- Select only the supported protocols that you that want the CSC SSM to scan. For example, if you do not want to scan HTTP traffic, be sure that service policies do not divert HTTP traffic to the CSC SSM.
- Select only those connections that risk trusted hosts protected by the security appliance. These are connections from outside or untrusted networks to inside networks. We recommend scanning the following connections:
  - Outbound HTTP connections.
  - FTP connections from clients inside the security appliance to servers outside the security appliance.
  - POP3 connections from clients inside the security appliance to servers outside the security appliance.
  - Incoming SMTP connections destined to inside mail servers.

FTP Scanning

The CSC SSM supports scanning of FTP file transfers only if the primary channel for the FTP session uses the standard port, which is TCP port 21.

FTP inspection must be enabled for the FTP traffic that you want scanned by the CSC SSM. This is because FTP uses a dynamically assigned secondary channel for data transfer. The security appliance determines the port assigned for the secondary channel and opens a pinhole to allow the data transfer to occur. If the CSC SSM is configured to scan FTP data, the security appliance diverts the data traffic to the CSC SSM.

You can apply FTP inspection either globally or to the same interface that the **csc** command is applied to. By default, FTP inspection is enabled globally. If you have not changed the default inspection configuration, no further FTP inspection configuration is required to enable FTP scanning by the CSC SSM.

For more information about FTP inspection or the default inspection configuration, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Examples

the security appliance should be configured to divert traffic to CSC SSM requests from clients on the inside network for HTTP, FTP, and POP3 connections to the outside network and incoming SMTP connections from outside hosts to the mail server on the DMZ network. HTTP requests from the inside network to the web server on the DMZ network should not be scanned.

The following configuration creates two service policies. The first policy, csc_out_policy, is applied to the inside interface and uses the csc_out access list to ensure that all outbound requests for FTP and POP3 are scanned. The csc_out access list also ensures that HTTP connections from inside to networks on the outside interface are scanned, but the access list includes a deny ACE to exclude HTTP connections from inside to servers on the DMZ network.

The second policy, csc_in_policy, is applied to the outside interface and uses the csc_in access list to ensure that requests for SMTP and HTTP originating on the outside interface and destined for the DMZ network are scanned by the CSC SSM. Scanning HTTP requests protects the web server from HTTP file uploads.

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

Note FTP inspection must be enabled for CSC SSM to scan files transferred by FTP. FTP inspection is enabled by default.

Related Commands

Commands	Description
class (policy-map)	Specifies a class map for traffic classification.
class-map	Creates a traffic classification map, for use with a policy map.
match port	Matches traffic using a destination port.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.

csd enable

To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in webvpn configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.

csd enable

no csd enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **csd enable** command does the following:

1. Provides a validity check that supplements the check performed by the previous **csd image** *path* command.
2. Creates an sdesktop folder on disk0: if one is not already present.
3. Inserts a data.xml (Cisco Secure Desktop configuration) file in the sdesktop folder if one is not already present.
4. Loads the data.xml from the flash device to the running configuration.
5. Enables Cisco Secure Desktop.

You can enter the **show webvpn csd** command to determine whether Cisco Secure Desktop is enabled.

The **csd image** *path* command must be in the running configuration before you enter the **csd enable** command.

The **no csd enable** command disables Cisco Secure Desktop in the running configuration. If Cisco Secure Desktop is disabled, you cannot access Cisco Secure Desktop Manager and remote users cannot use Cisco Secure Desktop.

If you transfer or replace the data.xml file, disable and then enable Cisco Secure Desktop to load the file into the running configuration.

Examples

The following example commands shows how to view the status of the Cisco Secure Desktop image and enable it:

```
hostname(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd	Identifies the version of Cisco Secure Desktop if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd image	Copies the Cisco Secure Desktop image named in the command, from the flash drive specified in the path to the running configuration.

csd image

To validate the Cisco Secure Desktop distribution package and add it to the running configuration, effectively installing Cisco Secure Desktop, use the **csd image** command in webvpn configuration mode. To remove the CSD distribution package from the running configuration, use the **no** form of the command:

csd image *path*

no csd image [*path*]

Syntax Description

path	Specifies the path and filename of the Cisco Secure Desktop package, up to 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Enter the **show webvpn csd** command to determine whether the Cisco Secure Desktop image is enabled before entering this command. The CLI indicates the version of Cisco Secure Desktop image that is currently installed if it is enabled.

Use the **csd image** command to install a new Cisco Secure Desktop image, or upgrade an existing image, after you download it from http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop to your computer, and transfer it to the flash drive. When downloading it, be sure to get the correct file for the security appliance; it is in the form **securedesktop_asa_**<*n*>**_**<*n*>***.pkg**.

Entering **no csd image** removes both management access to Cisco Secure Desktop Manager and remote user access to Cisco Secure Desktop. The security appliance does not make any changes to the Cisco Secure Desktop software and the Cisco Secure Desktop configuration on the flash drive when you enter this command.

Note Enter the **write memory** command to save the running configuration to ensure Cisco Secure Desktop is available the next time the security appliance reboots.

Examples

The following example commands show how to view the current Cisco Secure Desktop distribution package, view the contents of the flash file system, and upgrade to a new version:

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
hostname(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
hostname(config-webvpn)#
```

Related Commands

Command	Description
show webvpn csd	Identifies the version of Cisco Secure Desktop if it is enabled. Otherwise, the CLI indicates “Secure Desktop is not enabled.”
csd enable	Enables Cisco Secure Desktop for management and remote user access.

ctl

To enable the Certificate Trust List provider to parse the CTL file from the CTL client and install trustpoints, use the **ctl** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

ctl install

no ctl instal

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **ctl** command in CTL provider configuration mode to enable the CTL provider to parse the CTL file from the CTL client and install trustpoints for entries from the CTL file. Ttrustpoints installed by this command have names prefixed with "_internal_CTL_<ctl_name>." This command is optional and is enabled by default.

If this command is disabled, each CallManager server and CAPFs certificate must be manually imported and installed via the **crypto ca trustpoint** and **crypto ca certificate chain** commands.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

ctl-file (global)

To specify the CTL instance to create for the Phone Proxy or to parse the CTL file stored in Flash memory, use the **ctl-file** command in global configuration mode. To remove the CTL instance, use the **no** form of this command.

ctl-file *ctl_name* **noconfirm**

no ctl-file *ctl_name* **noconfirm**

Syntax Description

ctl_name	Specifies the name of the CTL instance.
noconfirm	(Optional) Used with the **no** command, stops warnings from being printed to the security appliance console about deleting trustpoints when the CTL file is removed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

If users have phones that require LSC provisioning, you must also import the CAPF certificate into the ASA from the CUMC when configuring the CTL file instance with the **ctl-file** command. See the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Note To create the CTL file use the **no shutdown** command in the ctl-file configuration mode. To modify or add entries to a CTL file or to delete a CTL file, use the **shutdown** command.

Using the **no** form of the command removes the CTL file and all enrolled trustpoints internally created by Phone Proxy. Additionally, removing the CTL file destroys all certificates received from the related Certificate Authority.

Examples

The following example shows the use of the **ctl-file** command to configure the CTL file for the Phone Proxy feature:

```
hostname(config)# ctl-file myctl
```

Related Commands

Command	Description
ctl-file (phone-proxy)	Specifies the CTL file to use when configuring the Phone Proxy instance.
cluster-ctl-file	Parses the CTL file stored in Flash memory to install the trustpoints from that file
phone-proxy	Configures the Phone Proxy instance.
record-entry	Specifies the trustpoints to be used for the creation of the CTL file.
sast	Specifies the number of SAST certificates to create in the CTL record.

ctl-file (phone-proxy)

To specify the CTL instance to use when configuring the Phone Proxy, use the **ctl-file** command in phone-proxy configuration mode. To remove the CTL instance, use the **no** form of this command.

ctl-file *ctl_name*

no ctl-file *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **ctl-file** command to configure the CTL file for the Phone Proxy feature:

```
hostname(config-phone-proxy)# ctl-file myctl
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
phone-proxy	Configures the Phone Proxy Instance.

ctl-provider

To configure a Certificate Trust List provider instance in CTL provider mode, use the **ctl-provider** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

Syntax Description

ctl_name	Specifies the name of the CTL provider instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **ctl-provider** command to enter CTL provider configuration mode to create a CTL provider instance.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.
export	Specifies the certificate to be exported to the client

Commands	Description
service	Specify the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

customization

To specify the customization to use for a tunnel-group, group, or user, use the **customization** command from the following modes:

In tunnel-group webvpn-attributes configuration mode and webvpn configuration mode (accessible from global configuration mode):

customization *name*

no customization *name*

In webvpn configuration mode (accessible from group-policy attributes configuration mode or username attributes configuration mode):

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

Syntax Description

name	Specifies the name of the WebVPN customization to apply.
none	Disables customization for the group or user, and displays the default WebVPN pages.
value *name*	Specifies the name of a customization to apply to the group policy or user.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn-attributes configuration	•	—	•	—	—
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Before entering the **customization** command in tunnel-group webvpn-attributes cofiguration mode, you must name and configure the customization using the **customization** command in webvpn configuration mode.

Mode-Dependent Command Options

The keywords available with the **customization** command differ depending on the mode you are in. In group-policy attributes > webvpn configuration mode and username attributes > webvpn configuration mode, the additional keywords **none** and **value** appear. The complete syntax from these modes is:

[**no**] **customization** {**none** | **value** *name*}

None disables customization for the group or user, and prevents the customization from being inherited. For example, if you enter the **customization none** command from username attributes > webvpn mode, the security appliance will not look for the value in the group policy or tunnel group.

name is the name of a customization to apply to the group or user.

To remove the command from the configuration, and cause the value to be inherited, use the **no** form of the command.

Examples

The following example shows a command sequence that first establishes a WebVPN customization named “123” that defines a password prompt. The example then defines a WebVPN tunnel group named “test” and uses the **customization** command to specifies the use of the WebVPN customization named “123”:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization 123
hostname(config-tunnel-webvpn)#
```

The next example shows the customization named “cisco” applied to the group policy named “cisco_sales”. Note that the additional command option **value** is required with the **customization** command entered in group-policy attributes > webvpn configuration mode:

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)#  webvpn
hostname(config-group-webvpn)# customization value cisco
```

Related Commands

Command	Description
clear configure tunnel-group	Removes all tunnel-group configuration.
show running-config tunnel-group	Displays the current tunnel-group configuration.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

CHAPTER 10

database path through debug xml Commands

database path

To specify a path or location for the local CA server database, use the **database** command in CA server configuration mode. To reset the path to flash memory, the default setting, use the **no** form of this command.

[no] database path *mount-name directory-path*

Syntax Description

directory-path	Specifies the path to a directory on the mount point where the CA files are stored.
mount-name	Specifies the mount name.

Defaults

By default, the CA server database is stored in flash memory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The local CA files stored in the database include the certificate database, user database files, temporary PKCS12 files, and the current CRL file. The *mount-name* is the same as the *name* argument for the **mount** command used to specify a file system for the security appliance.

Note These CA files are internal stored files and should not be modified.

Examples

The following example defines the mount point for the CA database as cifs_share. It also defines the database files directory on the mount point as ca_dir/files_dir.

```
hostname(config)# crypto ca server
hostname(config-ca-server)# database path cifs_share ca_dir/files_dir/
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows the user to configure and manage a local CA.
crypto ca server user-db write	Writes the user information configured in the local CA database to disk.
debug crypto ca server	Shows debug messages when the user configures the local CA server.
mount	Makes Common Internet File System (CIFS) and/or File Transfer Protocol (FTPFS) file systems accessible to the security appliance
show crypto ca server	Displays the characteristics of the CA configuration on the security appliance.
show crypto ca server cert-db	Displays the certificates issued by the CA server.

ddns (DDNS-update-method)

To specify a DDNS update method type, use the **ddns** command in DDNS-update-method mode. To remove an update method type from the running configuration, use the **no** form of this command.

ddns [**both**]

no ddns [**both**]

Syntax Description

both	(Optional) Specifies updating to both the DNS A and PTR resource records (RRs).

Defaults

Update only A RRs.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
DDNS-update-method	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Dynamic DNS (DDNS) updates the name to address and address to name mappings maintained by DNS. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.

Name and address mappings are contained in two types of resource records (RR):

- The A resource record contains domain name to IP address mappings.
- The PTR resource record contains IP address to domain name mappings.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

When issued in DDNS-update-method configuration mode, the **ddns** command defines whether the update is just to A RR, or to both A RR and PTR RR.

Examples

The following example configures updating to both the A and PTR RRs for the DDNS update method named ddns-2:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

Related Commands

Command	Description
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update (interface configuration)

To associate a dynamic DNS (DDNS) update method with a security appliance interface or an update hostname, use the **ddns update** command in interface configuration mode. To remove the association between the DDNS update method and the interface or the hostname from the running configuration, use the **no** form of this command.

ddns update [*method-name* | **hostname** *hostname*]

no ddns update [*method-name* | **hostname** *hostname*]

Syntax Description

hostname	Specifies that the next term in the command string is a hostname.
hostname	Specifies a hostname to be used for updates.
method-name	Specifies a method name for association with the interface being configured.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

After defining a DDNS update method, you must associate it with a security appliance interface to trigger DDNS updates.

A hostname could be a Fully Qualified Domain Name (FQDN) or just a hostname. If just a hostname, the security appliance appends a domain name to the hostname to create a FQDN.

Examples

The following example associates the interface GigabitEthernet0/2 with the DDNS update method named ddns-2 and the hostname hostname1.example.com:

```
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname hostname1.example.com
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

ddns update method (global configuration mode)

To create a method for dynamically updating a DNS resource records (RRs), use the **ddns update method** command in global configuration mode. To remove a dynamic DNS (DDNS) update method from the running configuration, use the **no** form of this command.

ddns update method *name*

no ddns update method *name*

Syntax Description

name	Specifies the name of a method for dynamically updating DNS records.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

DDNS updates the name to address and address to name mappings maintained by DNS. The update method configured by the **ddns update method** command determines what and how often dynamic DNS updates are performed. Of the two methods for performing DDNS updates—the IETF standard defined by RFC 2136 and a generic HTTP method—the security appliance supports the IETF method in this release.

Name and address mappings are contained in two types of resource records (RR):

- The A resource record contains domain name to IP address mappings.
- The PTR resource record contains IP address to domain name mappings.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

Note Before **ddns update method** will work, you must configure a reachable default DNS server using the **dns** command with domain lookup enabled on the interface.

Examples

The following example configures the DDNS update method named ddns-2:

```
hostname(config)# ddns update method ddns-2
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

debug aaa

To show debug messages for AAA, use the **debug aaa** command in privileged EXEC mode. To stop showing AAA messages, use the **no** form of this command.

debug aaa [**accounting** | **authentication** | **authorization** | **common** | **internal** | **vpn** [*level*]]

no debug aaa

Syntax Description

accounting	(Optional) Show debug messages for accounting only.
authentication	(Optional) Show debug messages for authentication only.
authorization	(Optional) Show debug messages for authorization only.
common	(Optional) Show debug messages for different states within the AAA feature.
internal	(Optional) Show debug messages for AAA functions supported by the local database only.
level	(Optional) Specifies the debug level. Valid with the **vpn** keyword only.
vpn	(Optional) Show debug messages for VPN-related AAA functions only.

Defaults

The default *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified to include new keywords.

Usage Guidelines

The **debug aaa** command displays detailed information about AAA activity. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables debugging for AAA functions supported by the local database:

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

Related Commands

Command	Description
show running-config aaa	Displays running configuration related to AAA.

debug appfw

To display detailed information about application inspection, use the **debug appfw** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

Syntax Description

chunk	(Optional) Displays runtime information about processing of chunked transfer encoded packets.
event	(Optional) Displays debug information about packet inspection events.
eventverb	(Optional) Displays the action taken by the security appliance in response to an event.
regex	(Optional) Displays information about matching patterns with predefined signatures.

Defaults

All options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug appfw** command displays detailed information about HTTP application inspection. The **no debug all** or **undebug all** commands turn off all enabled debug commands.

Examples

The following example enables the display of detailed information about application inspection:

```
hostname# debug appfw
```

Related Commands

Commands	Description
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.

debug arp

To show debug messages for ARP, use the **debug arp** command in privileged EXEC mode. To stop showing debug messages for ARP, use the **no** form of this command.

debug arp

no debug arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for ARP:

```
hostname# debug arp
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
show arp statistics	Shows ARP statistics.
show debug	Shows all enabled debuggers.

debug arp-inspection

To show debug messages for ARP inspection, use the **debug arp-inspection** command in privileged EXEC mode. To stop showing debug messages for ARP inspection, use the **no** form of this command.

debug arp-inspection

no debug arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for ARP inspection:

```
hostname# debug arp-inspection
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show debug	Shows all enabled debuggers.

debug asdm history

To view debug information for ASDM, use the **debug asdm history** command in privileged EXEC mode.

debug asdm history *level*

Syntax Description

level	(Optional) Specifies the debug level.

Defaults

The default *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **debug pdm history** command to the **debug asdm history** command.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables level 1 debugging of ASDM:

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

debug context

To show debug messages when you add or delete a security context, use the **debug context** command in privileged EXEC mode. To stop showing debug messages for contexts, use the **no** form of this command.

debug context [*level*]

no debug context [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for context management:

```
hostname# debug context
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows context information.
show debug	Shows all enabled debuggers.

debug cplane

To show debug messages about the control plane that connects internally to an SSM, use the **debug cplane** command in privileged EXEC mode. To stop showing debug messages for the control plane, use the **no** form of this command.

debug cplane [*level*]

no debug cplane [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for the control plane:

```
hostname# debug cplane
```

Related Commands

Command	Description
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.

Command	Description
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

debug crypto ca

To show debug messages for PKI activity (used with CAs), use the **debug crypto ca** command in privileged EXEC mode. To stop showing debug messages for PKI, use the **no** form of this command.

debug crypto ca [**messages** | **transactions**] [*level*]

no debug crypto ca [**messages** | **transactions**] [*level*]

Syntax Description

messages	(Optional) Shows only debug messages for PKI input and output messages.
transactions	(Optional) Shows only debug messages for PKI transactions.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Level 2 shows warnings. Level 3 shows informational messages. Levels 4 and up show additional information for troubleshooting.

Defaults

By default, this command shows all debug messages. The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for PKI:

```
hostname# debug crypto ca
```

Related Commands

Command	Description
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto ipsec	Shows debug messages for IPSec.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto ca server

To set the local CA server debug message level and begin listing associated debug messages, use the **debug crypto ca server** command in ca server configuration mode. To stop listing all debug messages, use the **no** form of the command.

debug crypto ca server [*level*]

no debug crypto ca server [*level*]

Syntax Description

level	Sets the debug message level to display, the range of values is between 1 and 255.

Defaults

The default debug level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks. Levels 5 and higher are reserved for raw data dumps and should be avoided during normal debugging because of excessive debug output.

Examples

The following example sets the debug level to 3:

```
hostname(config-ca-server)# debug crypto ca server 3
hostname(config-ca-server)#
```

The following example turns off all debugging:

```
hostname(config-ca-server)# no debug crypto ca server
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list (CRL) distribution point (CDP) to be include in the certificates issued by the CA.
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
database path	Specifies a path or location for the local CA server database.
show crypto ca server	Displays the characteristics of the certificate authority configuration on the security appliance in ASCII text format.
show crypto ca server certificate	Displays the local CA configuration in base64 format.
show crypto ca server crl	Displays the current CRL of the local CA.

debug crypto engine

To show debug messages for the crypto engine, use the **debug crypto engine** command in privileged EXEC mode. To stop showing debug messages for the crypto engine, use the **no** form of this command.

debug crypto engine [*level*]

no debug crypto engine [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for the crypto engine:

```
hostname# debug crypto engine
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto ipsec	Shows debug messages for IPSec.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto ipsec

To show debug messages for IPSec, use the **debug crypto ipsec** command in privileged EXEC mode. To stop showing debug messages for IPSec, use the **no** form of this command.

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for IPSec:

```
hostname# debug crypto ipsec
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto isakmp	Shows debug messages for ISAKMP.

debug crypto isakmp

To show debug messages for ISAKMP, use the **debug crypto isakmp** command in privileged EXEC mode. To stop showing debug messages for ISAKMP, use the **no** form of this command.

debug crypto isakmp [**timers**] [*level*]

no debug crypto isakmp [**timers**] [*level*]

Syntax Description

timers	(Optional) Shows debug messages for ISAKMP timer expiration.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number. Level 1 (the default) shows messages only when errors occur. Levels 2 through 7 show additional information. Level 254 shows decrypted ISAKMP packets in a human readable format. Level 255 shows hexadecimal dumps of decrypted ISAKMP packets.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for ISAKMP:

```
hostname# debug crypto isakmp
```

Related Commands

Command	Description
debug crypto ca	Shows debug messages for the CA.
debug crypto engine	Shows debug messages for the crypto engine.
debug crypto ipsec	Shows debug messages for IPSec.

debug ctiqbe

To show debug messages for CTIQBE application inspection, use the **debug ctiqbe** command in privileged EXEC mode. To stop showing debug messages for CTIQBE application inspection, use the **no** form of this command.

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug ctiqbe** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for CTIQBE application inspection:

```
hostname# debug ctiqbe
```

Related Commands

Command	Description
inspect ctiqbe	Enables CTIQBE application inspection.
show ctiqbe	Displays information about CTIQBE sessions established through the security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug ctl-provider

To show debug messages for Certificate Trust List providers, use the **debug ctl-provider** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug ctl-provider [**errors** | **events** | **parser**]

no debug ctl-provider [**errors** | **events** | **parser**]

Syntax Description

errors	Specifies CTL provider error debugging.
events	Specifies CTL provider event debugging.
parser	Specifies CTL provider parser debugging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for CTL provider:

```
hostname# debug ctl-provider
```

Related Commands

Command	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.

debug dap

To enable logging of Dynamic Access Policy events, use the **debug dap** command in privileged EXEC mode. To disable the logging of DAP debug messages, use the **no** form of this command.

debug dap {errors | trace}

no debug dap [errors | trace]

Syntax Description

errors	Specifies DAP processing errors.
trace	Specifies a DAP function trace.

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The high priority assigned to debugging output can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example shows how to enable DAP trace debugging:

```
hostname # debug dap trace
hostname #
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.

debug ddns

To show debug messages for DDNS, use the **debug ddns** command in privileged EXEC mode. To disable debug messages, use the **no** form of this command.

debug ddns

no debug ddns

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **debug ddns** command displays detailed information about DDNS. The **undebug ddns** turns off DDNS debugging information as does the **no debug ddns** command.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows an example of enabling DDNS debug messages:

```
hostname# debug ddns
debug ddns enabled at level 1
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a DDNS update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

debug dhcpc

To enable debugging of the DHCP client, use the **debug dhcpc** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpc {**detail** | **packet** | **error**} [*level*]

no debug dhcpc {**detail** | **packet** | **error**} [*level*]

Syntax Description

detail	Displays detail event information that is associated with the DHCP client.
error	Displays error messages that are associated with the DHCP client.
level	(Optional) Specifies the debug level. Valid valuse range from 1 to 255.
packet	Displays packet information that is associated with the DHCP client.

Defaults

The default debug level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Displays DHCP client debug information.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows how to enable debugging for the DHCP client:

```
hostname# debug dhcpc detail 5
debug dhcpc detail enabled at level 5
```

Related Commands

Command	Description
show ip address dhcp	Displays detailed information about the DHCP lease for an interface.
show running-config interface	Displays the running configuration of the specified interface.

debug dhcpd

To enable debugging of the DHCP server, use the **debug dhcpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpd {**event** | **packet**} [*level*]

no debug dhcpd {**event** | **packet**} [*level*]

Syntax Description

event	Displays event information that is associated with the DHCP server.
level	(Optional) Specifies the debug level. Valid valuse range from 1 to 255.
packet	Displays packet information that is associated with the DHCP server.

Defaults

The default debug level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **debug dhcpd event** command displays event information about the DHCP server. The **debug dhcpd packet** command displays packet information about the DHCP server.

Use the **no** form of the d**ebug dhcpd** commands to disable debugging.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows an example of enabling DHCP event debugging:

```
hostname# debug dhcpd event
debug dhcpd event enabled at level 1
```

Related Commands

Command	Description
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

debug dhcpd ddns

To enable debugging of the DHCP DDNS, use the **debug dhcpd ddns** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpd ddns [*level*]

no debug dhcpd ddns [*level*]

Syntax Description

level	(Optional) Specifies the debug level. Valid values range from 1 to 255.

Defaults

The default debug level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **debug dhcpd ddns** command displays detailed information about DHCP and DDNS. The **undebug dhcpd ddns** command turns off DHCP and DDNS debugging information as does the **no debug dhcpd ddns** command.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows DHCP DDNS debugging being enabled:

```
hostname# debug dhcpd ddns
debug dhcpd ddns enabled at level 1
```

Related Commands

Command	Description
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.
show running-config dhcpd	Displays the current DHCP server configuration.
show running-config ddns	Display the DDNS update methods of the running configuration.

debug dhcprelay

To enable debugging of the DHCP relay server, use the **debug dhcpreleay** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcprelay {**event** | **packet** | **error**} [*level*]

no debug dhcprelay {**event** | **packet** | **error**} [*level*]

Syntax Description

error	Displays error messages that are associated with the DHCP relay agent.
event	Displays event information that is associated with the DHCP relay agent.
level	(Optional) Specifies the debug level. Valid valuse range from 1 to 255.
packet	Displays packet information that is associated with the DHCP relay agent.

Defaults

The default debug level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows how to enable debugging for DHCP relay agent error messages:

```
hostname# debug dhcprelay error
debug dhcprelay error enabled at level 1
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
show dhcprelay statistics	Displays DHCP relay agent statistic information.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

debug disk

To display file system debug information, use the **debug disk** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug disk {**file** | **file-verbose** | **filesystem**} [*level*]

no debug disk {**file** | **file-verbose** | **filesystem**}

Syntax Description

file	Enables file-level disk debug messages.
file-verbose	Enables verbose file-level disk debug messages
filesystem	Enables file system debug messages.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables file-level disk debug messages. The **show debug** command reveals that file-level disk debug messages are enabled. The **dir** command causes several debug messages.

```
hostname# debug disk file
debug disk file enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname# dir
```

```
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3

Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0

4      -rw-  5124096     14:42:27 Apr 04 2005  cdisk.binIFS: Opened: file flash:/ as fd 3

9      -rw-  5919340     14:53:39 Apr 04 2005  ASDMIFS: Getdent: fd 3

11     drw-  0           15:18:56 Apr 21 2005  syslog
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3

16128000 bytes total (5047296 bytes free)
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug dns

To show debug messages for DNS, use the **debug dns** command in privileged EXEC mode. To stop showing debug messages for DNS, use the **no** form of this command.

debug dns [**resolver** | **all**] [*level*]

no debug dns [**resolver** | **all**] [*level*]

Syntax Description

all	(Default) Shows all messages, including messages about the DNS cache.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
resolver	(Optional) Shows only DNS resolver messages.

Defaults

The default level is 1. If you do not specify any keywords, the security appliance shows all mesages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for DNS:

```
hostname# debug dns
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect dns	Enables DNS application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug eap

To enable logging of EAP events to debug NAC messaging, use the **debug eap** command in privileged EXEC mode. To disable the logging of EAP debug messages, use the **no** form of this command.

debug eap {**all** | **errors** | **events** | **packets** | **sm**}

no debug eap [**all** | **errors** | **events** | **packets** | **sm**]

Syntax Description

all	Enables logging of debug messages about all EAP information.
errors	Enables logging of EAP packet errors.
events	Enables logging of EAP session events.
packets	Enables logging of debug messages about EAP packet information.
sm	Enables logging of debug messages about EAP state machine information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the security appliance records EAP session state changes and EAP status query events, and generates a complete record of EAP and packet contents in hexadecimal format.

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the logging of all EAP session events:

```
hostname# debug eap events
hostname#
```

The following example enables the logging of all EAP debug messages:

```
hostname# debug eap all
hostname#
```

The following example disables the logging of all EAP debug messages:

```
hostname# no debug eap
hostname#
```

Related Commands

Command	Description
debug eou	Enables logging of EAPoUDP events to debug NAC messaging.
debug nac	Enables logging of NAC events.
eou initialize	Clears the resources assigned to one or more NAC sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC sessions.
show debug	Displays current debug configuration.

debug eigrp fsm

To display debug information the DUAL finite state machine, use the **debug eigrp fsm** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp fsm

no debug eigrp fsm

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command lets you observe EIGRP feasible successor activity and to determine whether route updates are being installed and deleted by the routing process.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug eigrp fsm** command:

```
hostname# debug eigrp fsm

DUAL: dual_rcvupdate(): 172.25.166.0 255.255.255.0 via 0.0.0.0 metric 750080/0
DUAL: Find FS for dest 172.25.166.0 255.255.255.0. FD is 4294967295, RD is 4294967295
found
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
DUAL: dual_rcvupdate(): 192.168.4.0 255.255.255.0 via 0.0.0.0 metric 4294967295/4294967295
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
```

```
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

In the fist line, DUAL stands for diffusing update algorithm. It is the basic mechanism within EIGRP that makes the routing decisions. The next three fields are the Internet address and mask of the destination network and the address through which the update was received. The metric field shows the metric stored in the routing table and the metric advertised by the neighbor sending the information. If shown, the term “Metric... inaccessible” usually means that the neighbor router no longer has a route to the destination, or the destination is in a hold-down state.

In the following output, EIGRP is attempting to find a feasible successor for the destination. Feasible successors are part of the DUAL loop avoidance methods. The FD field contains more loop avoidance state information. The RD field is the reported distance, which is the metric used in update, query, or reply packets.

The indented line with the “not found” message means a feasible successor was not found for 192.168.4.0 and EIGRP must start a diffusing computation. This means it begins to actively probe (sends query packets about destination 192.168.4.0) the network looking for alternate paths to 192.164.4.0.

```
DUAL: Find FS for dest 192.168.4.0 255.255.255.0. FD is 2249216, RD is 2249216
DUAL:   0.0.0.0 metric 4294967295/4294967295not found Dmin is 4294967295
```

The following output indicates the route DUAL successfully installed into the routing table:

```
DUAL: RT installed 172.25.166.0 255.255.255.0 via 0.0.0.0
```

The following output shows that no routes to the destination were discovered and that the route information is being removed from the topology table:

```
DUAL: Dest 192.168.4.0 255.255.255.0 not entering active state.
DUAL: Removing dest 192.168.4.0 255.255.255.0, nexthop 0.0.0.0
DUAL: No routes. Flushing dest 192.168.4.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp topology	Displays the EIGRP topology table.

debug eigrp neighbors

To display debug information for neighbors discovered by EIGRP, use the **debug eigrp neighbors** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp neighbors [**siatimer** | **static**]

no debug eigrp neighbors [**siatimer** | **static**]

Syntax Description

siatimer	(Optional) Displays EIGRP stuck in active messages.
static	(Optional) Displays EIGRP static neighbor messages.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug eigrp neighbors static** command. The example shows a static neighbor being added, and then removed, and the corresponding debug messages.

```
hostname# debug eigrp neighbors static

EIGRP Static Neighbors debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Multicast Hello is disabled on Ethernet0/0!
```

```
EIGRP: Add new static nbr 10.86.194.3 to AS 100 Ethernet0/0

hostname(config-router)# no neighbor 10.86.194.3 interface outside
hostname(config-router)#

EIGRP: Static nbr 10.86.194.3 not in AS 100 Ethernet0/0 dynamic list
EIGRP: Delete static nbr 10.86.194.3 from AS 100 Ethernet0/0
EIGRP: Multicast Hello is enabled on Ethernet0/0!

hostname(config-router)# no debug eigrp neighbors static

EIGRP Static Neighbors debugging is off
```

Related Commands

Command	Description
neighbor	Defines an EIGRP neighbor.
show eigrp neighbors	Displays the EIGRP neighbor table.

debug eigrp packets

To display debug information for EIGRP packets, use the **debug eigrp packets** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

no debug eigrp packets [**SIAquery** | **SIAreply** | **ack** | **hello** | **probe** | **query** | **reply** | **request** | **retry** | **stub** | **terse** | **update** | **verbose**]

Syntax Description

ack	(Optional) Limits the debug output to EIGRP ack packets.
hello	(Optional) Limits the debug output to EIGRP hello packets.
probe	(Optional) Limits the debug output to EIGRP probe packets.
query	(Optional) Limits the debug output to EIGRP query packets.
reply	(Optional) Limits the debug output to EIGRP reply packets.
request	(Optional) Limits the debug output to EIGRP request packets.
retry	(Optional) Limits the debug output to EIGRP retry packets.
SIAquery	(Optional) Limits the debug output to EIGRP stuck in active query packets.
SIAreply	(Optional) Limits the debug output to EIGRP stuck in active reply packets.
stub	(Optional) Limits the debug output to EIGRP stub routing packets.
terse	(Optional) Displays all EIGRP packets except hello packets.
update	(Optional) Limits the debug output to EIGRP update packets.
verbose	(Optional) Outputs all packet debug messages.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can specify more than one packet type in a single command, for example:

```
debug eigrp packets query reply
```

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug eigrp packets** command:

```
hostname# debug eigrp packets

EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Sending HELLO on Ethernet0/1
       AS 109, Flags 0x0, Seq 0, Ack 0
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x1, Seq 1, Ack 0
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Sending HELLO/ACK on Ethernet0/1 to 192.195.78.24,
       AS 109, Flags 0x0, Seq 0, Ack 1
EIGRP: Received UPDATE on Ethernet0/1 from 192.195.78.24,
       AS 109, Flags 0x0, Seq 2, Ack 0
```

The output shows transmission and receipt of EIGRP packets. The sequence and acknowledgment numbers used by the EIGRP reliable transport algorithm are shown in the output. Where applicable, the network-layer address of the neighboring router is also included.

Related Commands

Command	Description
show eigrp traffic	Displays the number of EIGRP packets sent and received.

debug eigrp transmit

To display transmittal messages sent by EIGRP, use the **debug eigrp transmit** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

no debug eigrp transmit [**ack**] [**build**] [**detail**] [**link**] [**packetize**] [**peerdown**] [**sia**] [**startup**] [**strange**]

Syntax Description

ack	(Optional) Information for acknowledgment (ACK) messages sent by the system.
build	(Optional) Build information messages (messages that indicate that a topology table was either successfully built or could not be built).
detail	(Optional) Additional detail for debug output.
link	(Optional) Information regarding topology table linked-list management.
packetize	(Optional) Information regarding packetize events.
peerdown	(Optional) Information regarding the impact on packet generation when a peer is down.
sia	(Optional) Stuck-in-active messages.
startup	(Optional) Information regarding peer startup and initialization packets that have been transmitted.
strange	(Optional) Unusual events relating to packet processing.

Defaults

If at least one transmittal event is not specified, all transmittal events are shown in the debug output.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can specify more than one transmittal event in a single command, For example:

```
hostname# debug eigrp ack build link
```

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug eigrp transmit** command. The example shows a **network** command being entered and the transmittal event debug message that is generated.

```
hostname# debug eigrp transmit

EIGRP Transmission Events debugging is on

    (ACK, PACKETIZE, STARTUP, PEERDOWN, LINK, BUILD, STRANGE, SIA, DETAIL)

hostname# configure terminal
hostname(config)# router eigrp 100
hostname(config-router)# network 10.86.194.0 255.255.255.0

DNDB UPDATE 10.86.194.0 255.255.255.0, serno 0 to 1, refcount 0

hostname(config-router)# no debug eigrp transmit

EIGRP Transmission Events debugging is off
```

Related Commands

Command	Description
show eigrp traffic	Displays the number of EIGRP packets sent and received.

debug eigrp user-interface

To display debug information for EIGRP user events, use the **debug eigrp user-interface** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug eigrp user-interface

no debug eigrp user-interface

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug eigrp user-interface** command. The output is caused by an administrator removing a **passive-interface** command from an EIGRP configuration.

```
hostname# debug eigrp user-interface

EIGRP UI Events debugging is on

hostname# configure terminal
hostname(config) router eigrp 100
hostname(config-router)# no passive-interface inside

CSB2AF: FOUND (AS=100, Name=, VRF=0, AFI=ipv4)

hostname(config-router)# no debug eigrp user-interface

EIGRP UI Events debugging is off
```

Related Commands

Command	Description
router eigrp	Enables an EIGRP routing process and enters router configuration mode.
show running-config eigrp	Displays the EIGRP commands in the running configuration.

debug entity

To display MIB debug information, use the **debug entity** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug entity [*level*]

no debug entity

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables MIB debug messages. The **show debug** command reveals that MIB debug messages are enabled.

```
hostname# debug entity
debug entity  enabled at level 1
hostname# show debug
debug entity  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug eou

To enable logging of EAPoUDP events to debug NAC messaging, use the **debug eou** command in privileged EXEC mode. To disable the logging of EAPoUDP debug messages, use the **no** form of this command.

debug eou {**all** | **eap** | **errors** | **events** | **packets** | **sm**}

no debug eou [**all** | **eap** | **errors** | **events** | **packets** | **sm**]

Syntax Description

all	Enables logging of debug messages about all EAPoUDP information.
eap	Enables logging of debug messages about EAPoUDP packets.
errors	Enables logging of EAPoUDP packet errors.
events	Enables logging of EAPoUDP session events.
packets	Enables logging of debug messages about EAPoUDP packet information.
sm	Enables logging of debug messages about EAPoUDP state machine information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the security appliance records EAPoUDP session state changes and timer events, and generates a complete record of EAPoUDP header and packet contents in hexadecimal format.

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the logging of all EAPoUDP session events:

```
hostname# debug eou events
```

```
hostname#
```

The following example enables the logging of all EAPoUDP debug messages:

```
hostname# debug eou all
hostname#
```

The following example disables the logging of all EAPoUDP debug messages:

```
hostname# no debug eou
hostname#
```

Related Commands

Command	Description
debug eap	Enables logging of EAP events to debug NAC messaging.
debug nac	Enables logging of NAC events.
eou initialize	Clears the resources assigned to one or more NAC sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC sessions.
show debug	Displays current debug configuration.

debug esmtp

To show debug messages for SMTP/ESMTP application inspection, use the **debug esmtp** command in privileged EXEC mode. To stop showing debug messages for SMTP/ESMTP application inspection, use the **no** form of this command.

debug esmtp [*level*]

no debug esmtp [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug esmtp** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for SMTP/ESMTP application inspection:

```
hostname# debug esmtp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect esmtp	Enables ESMTP application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

debug fixup

To display detailed information about application inspection, use the **debug fixup** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug fixup

no debug fixup

Defaults

All options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **debug fixup** command displays detailed information about application inspection. The **no debug all** or **undebug all** commands turn off all enabled debug commands.

Examples

The following example enables the display of detailed information about application inspection:

```
hostname# debug fixup
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect *protocol*	Enables application inspection for specific protocols.
policy-map	Associates a class map with specific security actions.

debug fover

To display failover debug information, use the **debug fover** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fover {**cable** | **cmd-exec** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdmp** | **rxip** | **switch** | **sync** | **tx** | **txdmp** | **txip** | **verify**}

no debug fover {**cable** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdmp** | **rxip** | **switch** | **sync** | **tx** | **txdmp** | **txip** | **verify**}

Syntax Description

cable	Failover LAN status or serial cable status.
cmd-exec	**failover exec** command execution trace.
fail	Failover internal exception.
fmsg	Failover message.
ifc	Network interface status trace.
open	Failover device open.
rx	Failover message receive.
rxdmp	Failover receive message dump (serial console only).
rxip	IP network failover packet receive.
switch	Failover switching status.
sync	Failover configuration/command replication.
tx	Failover message transmit.
txdmp	Failover transmit message dump (serial console only).
txip	IP network failover packet transmit.
verify	Failover message verify.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified. It includes additional debug keywords.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug fover cmd-exec** command. After debugging is enabled, a **failover exec** command is entered. The results of the **failover exec** command is shown after the debug output.

```
hostname(config)# debug fover cmd-exec

fover event trace on

hostname(config)# failover exec mate show running-config failover

ci/console: Sending cmd: show runn failovero to peer for execution, seq = 4
ci/console: frep_execv_cmd: replicating exec cmd: show runn failover...
fover_parse: Fover rexec response: seq=4, size=228, data="fail..."
ci/console: Fover rexec waiting at clock tick 2670960
fover_parse: Fover rexec ack: seq = 4, ret_val = 0
ci/console: Fover rexec conteinuer at clock tick: 2671040
ci/console: Fover exec succeeded, seq = 5

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover key *****
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

Related Commands

Command	Description
show failover	Displays information about the failover configuration and operational statistics.

debug fsm

To display FSM debug information, use the **debug fsm** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug fsm [*level*]

no debug fsm

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables FSM debug messages. The **show debug** command reveals that FSM debug messages are enabled.

```
hostname# debug fsm
debug fsm  enabled at level 1
hostname# show debug
debug fsm  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug ftp client

To show debug messages for FTP, use the **debug ftp client** command in privileged EXEC mode. To stop showing debug messages for FTP, use the **no** form of this command.

debug ftp client [*level*]

no debug ftp client [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug ftp client** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for FTP:

```
hostname# debug ftp client
```

Related Commands

Command	Description
copy	Uploads or downloads image files or configuration files to or from an FTP server.
ftp mode passive	Configures the mode for FTP sessions.
show running-config ftp mode	Displays FTP client configuration.

debug generic

To display miscellaneous debug information, use the **debug generic** command in privileged EXEC mode. To disable the display of miscellaneous debug information, use the **no** form of this command.

debug generic [*level*]

no debug generic

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables miscellaneous debug messages. The **show debug** command reveals that miscellaneous debug messages are enabled.

```
hostname# debug generic
debug generic  enabled at level 1
hostname# show debug
debug generic  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug gtp

To display detailed information about GTP inspection, use the **debug gtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug gtp {**error** | **event** | **ha** | **parser**}

no debug gtp {**error** | **event** | **ha** | **parser**}

Syntax Description

error	Displays debug information on errors encountered while processing the GTP message.
event	Displays debug information on GTP events.
ha option	Debugs information on GTP HA events.
parser	Displays debug information for parsing the GTP messages.

Defaults

All options are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug gtp** command displays detailed information about GTP inspection. The **no debug all** or **undebug all** commands turn off all enabled debug commands.

Note GTP inspection requires a special license.

Examples

The following example enables the display of detailed information about GTP inspection:

```
hostname# debug gtp
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.
show running-config gtp-map	Shows the GTP maps that have been configured.

debug h323

To show debug messages for H.323, use the **debug h323** command in privileged EXEC mode. To stop showing debug messages for H.323, use the **no** form of this command.

debug h323 {h225 | h245 | ras} [asn | event]

no debug h323 {h225 | h245 | ras} [asn | event]

Syntax Description

h225	Specifies H.225 signaling.
h245	Specifies H.245 signaling.
ras	Specifies the registration, admission, and status protocol.
asn	(Optional) Displays the output of the decoded protocol data units (PDU)s.
event	(Optional) Displays the signaling events or turns on both traces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug h323** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for H.225 signaling:

```
hostname# debug h323 h225
```

Related Commands

Command	Description
inspect h323	Enables H.323 application inspection.
show h225	Displays information for H.225 sessions established across the security appliance.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | **h323**	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

debug http

To display detailed information about HTTP traffic, use the **debug http** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug http [*level*]

no debug http [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The defafult for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **debug http** command displays detailed information about HTTP traffic. The **no debug all** or **undebug all** commands turn off all enabled debug commands.

Examples

The following example enables the display of detailed information about HTTP traffic:

```
hostname# debug http
```

Related Commands

Commands	Description
http	Specifies hosts that can access the HTTP server internal to the security appliance.
http-proxy	Configures an HTTP proxy server.
http redirect	Redirects HTTP traffic to HTTPS.
http server enable	Enables the security appliance HTTP server.

debug http-map

To show debug messages for HTTP application inspection maps, use the **debug http-map** command in privileged EXEC mode. To stop showing debug messages for HTTP application inspection, use the **no** form of this command.

debug http-map

no debug http-map

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug http-map** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for HTTP application inspection:

```
hostname# debug http-map
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

debug icmp

To display detailed information about ICMP inspection, use the **debug icmp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug icmp trace [*level*]

no debug icmp trace [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.
trace	Displays debug information about ICMP trace activity.

Defaults

All options are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **debug icmp** command displays detailed information about ICMP inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables the display of detailed information about ICMP inspection:

```
hostname# debug icmp
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
show conn	Displays the state of connections through the security appliance for different protocols and session types.

Commands	Description
show icmp	Displays ICMP configuration.
timeout icmp	Configures idle timeout for ICMP.

debug igmp

To display IGMP debug information, use the **debug igmp** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

debug igmp [**group** *group_id* | **interface** *if_name*]

no debug igmp [**group** *group_id* | **interface** *if_name*]

Syntax Description

group *group_id*	Displays IGMP debug information for the specified group.
interface *if_name*	Display IGMP debug information for the specified interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug igmp** command:

```
hostname#debug igmp

IGMP debugging is on
IGMP: Received v2 Query on outside from 192.168.3.2
IGMP: Send v2 general Query on dmz
IGMP: Received v2 Query on dmz from 192.168.4.1
IGMP: Send v2 general Query on outside
IGMP: Received v2 Query on outside from 192.168.3.1
IGMP: Send v2 general Query on inside
IGMP: Received v2 Query on inside from 192.168.1.1
IGMP: Received v2 Report on inside from 192.168.1.6 for 224.1.1.1
IGMP: Updating EXCLUDE group timer for 224.1.1.1
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

debug ils

To show debug messages for ILS, use the **debug ils** command in privileged EXEC mode. To stop showing debug messages for ILS, use the **no** form of this command.

debug ils [*level*]

no debug ils [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug ils** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for ILS application inspection:

```
hostname# debug ils
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ils	Enables ILS application inspection.

Command	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

Related Commands

debug imagemgr

To display Image Manager debug information, use the **debug imagemgr** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug imagemgr [*level*]

no debug imagemgr

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables Image Manager debug messages. The **show debug** command reveals that Image Manager debug messages are enabled.

```
hostname# debug imagemgr
debug imagemgr  enabled at level 1
hostname# show debug
debug imagemgr  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug inspect tls-proxy

To show debug messages for TLS proxy inspection, use the **debug inspect tls-proxy** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

no debug inspect tls-proxy [**all** | **errors** | **events** | **packets**]

Syntax Description

all	Specifies all TLS proxy debugging.
errors	Specifies TLS proxy error debugging.
events	Specifies TLS proxy event debugging.
packets	Specifies TLS proxy packet debugging.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for TLS proxy:

```
hostname# debug inspect tls-proxy
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

debug ip eigrp

To display debug information EIGRP protocol packets, use the **debug ip eigrp** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

no debug ip eigrp [*as-number*] [*ip-addr mask* | **neighbor** *nbr-addr* | **notifications** | **summary**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.
ip-addr mask	(Optional) Limits debug output to messages that fall within the range defined by the IP address and network mask.
neighbor *nbr-addr*	(Optional) Limits debug output to the specified neighbor.
notifications	(Optional) Limits debug output to EIGRP protocol events and notifications.
summary	(Optional) Limits debug output to summary route processing.
user-interface	(Optional) Limits debug output to user events.

Defaults

If no keywords or arguments are specified, only debug messages from the IPv4 ASDM are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command helps you analyze the packets that are sent and received on an interface.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ip eigrp** command:

```
hostname# debug ip eigrp

IP-EIGRP Route Events debugging is on

EIGRP-IPv4(Default-IP-Routing-Table:1): Processing incoming UPDATE packet
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.0.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.168.3.0 255.255.255.0 M 386560 - 256000
130560 SM 360960 - 256000 104960
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.43.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.43.0 255.255.255.0 metric 371200 -
256000 115200
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.246.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.246.0 255.255.255.0 metric 46310656 -
45714176 596480
EIGRP-IPv4(Default-IP-Routing-Table:1): 172.69.40.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 172.69.40.0 255.255.255.0 metric 2272256 -
1657856 614400
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.245.0 255.255.255.0, - do advertise out
Ethernet0/1
EIGRP-IPv4(Default-IP-Routing-Table:1): Ext 192.135.245.0 255.255.255.0 metric 40622080 -
40000000 622080
EIGRP-IPv4(Default-IP-Routing-Table:1): 192.135.244.0 255.255.255.0, - do advertise out
Ethernet0/1
```

Table 10-1describes the significant fields shown in the display.

Table 10-1 debug ip eigrp Field Descriptions

Field	Description
IP-EIGRP:	Indicates IP EIGRP messages.
Ext	Indicates that the following address is an external route rather than an internal route, which would be labeled as Int.
M	Displays the computed metric, which includes the value in the SM field and the cost between this router and the neighbor. The first number is the composite metric. The next two numbers are the inverse bandwidth and the delay, respectively.
SM	Displays the metric as reported by the neighbor.

Related Commands

Command	Description
debug eigrp packets	Displays debug information for EIGRP packets.

debug ipsec-over-tcp

To display IPSec-over-TCP debug information, use the **debug ipsec-over-tcp** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables IPSec-over-TCP debug messages. The **show debug** command reveals that IPSec-over-TCP debug messages are enabled.

```
hostname# debug ipsec-over-tcp
debug ipsec-over-tcp  enabled at level 1
hostname# show debug
debug ipsec-over-tcp  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug ipv6

To display ipv6 debug messages, use the **debug ipv6** command in privileged EXEC mode. To stop the display of debug messages, use the **no** form of this command.

debug ipv6 {icmp | **interface** | **mld** | **nd** | **packet** | **routing**}

no debug ipv6 {icmp | **interface** | **nd** | **packet** | **routing**}

Syntax Description

icmp	Displays debug messages for IPv6 ICMP transactions, excluding ICMPv6 neighbor discovery transactions.
interface	Displays debug information for IPv6 interfaces.
mld	Displays debug messages for Multicast Listener Discovery (MLD).
nd	Displays debug messages for ICMPv6 neighbor discovery transactions.
packet	Displays debug messages for IPv6 packets.
routing	Displays debug messages for IPv6 routing table updates and route cache updates.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output for the **debug ipv6 icmp** command:

```
hostname# debug ipv6 icmp
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
```

```
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

Related Commands

Command	Description
ipv6 icmp	Defines access rules for ICMP messages that terminate on a security appliance interface.
ipv6 address	Configures an interface with an IPv6 address or addresses.
ipv6 nd dad attempts	Defines the number of neighbor discovery attempts performed during duplicate address detection.
ipv6 route	Defines a static entry in the IPv6 routing table.

debug iua-proxy

To display IUA proxy debug information, use the **debug iua-proxy** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug iua-proxy [*level*]

no debug iua-proxy

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables IUA-proxy debug messages. The **show debug** command reveals that IUA-proxy debug messages are enabled.

```
hostname# debug iua-proxy
debug iua-proxy  enabled at level 1
hostname# show debug
debug iua-proxy  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug kerberos

To display Kerberos authentication debug information, use the **debug kerberos** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug kerberos [*level*]

no debug kerberos

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables Kerberos debug messages. The **show debug** command reveals that Kerberos debug messages are enabled.

```
hostname# debug kerberos
debug kerberos  enabled at level 1
hostname# show debug
debug kerberos  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug l2tp

To display L2TP debug information, use the **debug l2tp** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug l2tp {**data** | **error** | **event** | **packet**} *level*

no debug l2tp {**data** | **error** | **event** | **packet**} *level*

Syntax Description

data	displays data packet trace information.
error	Displays error events.
event	Displays L2TP connection events.
packet	Displays packet trace information.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables L2TP debug messages for connection events. The **show debug** command reveals that L2TP debug messages are enabled.

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug ldap

To display LDAP debug information, use the **debug ldap** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ldap [*level*]

no debug ldap

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables LDAP debug messages. The **show debug** command reveals that LDAP debug messages are enabled.

```
hostname# debug ldap
debug ldap  enabled at level 1
hostname# show debug
debug ldap  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug mac-address-table

To show debug messages for the MAC address table, use the **debug mac-address-table** command in privileged EXEC mode. To stop showing debug messages for the MAC address table, use the **no** form of this command.

debug mac-address-table [*level*]

no debug mac-address-table [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for the MAC address table:

```
hostname# debug mac-address-table
```

Related Commands

Command	Description
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.

Command	Description
show debug	Shows all enabled debuggers.
show mac-address-table	Shows MAC address table entries.

debug menu

To display detailed debug information for specific features, use the **debug menu** command in privileged EXEC mode.

debug menu

Caution The **debug menu** command should be used only under the supervision of Cisco TAC.

Syntax Description

This command should be used only under the supervision of Cisco TAC.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

This command should be used only under the supervision of Cisco TAC.

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug mfib

To display MFIB debug information, use the **debug mfib** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*]

no debug mfib {**db** | **init** | **mrib** | **pak** | **ps** | **signal**} [*group*]

Syntax Description

db	(Optional) Displays debug information for route database operations.
group	(Optional) IP address of the multicast group.
init	(Optional) Displays system initialization activity.
mrib	(Optional) Displays debug information for communication with MFIB.
pak	(Optional) Displays debug information for packet forwarding operations.
ps	(Optional) Displays debug information for process switching operations.
signal	(Optional) Displays debug information for MFIB signaling to routing protocols.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example displays MFIB dabase operation debug information:

```
hostname# debug mfib db
MFIB IPv4 db debugging enabled
```

Related Commands

Command	Description
show mfib	Displays MFIB forwarding entries and interfaces.

debug mgcp

To display detailed information about MGCP application inspection, use the **debug mgcp** command in privileged EXEC mode. To disable debugging, Use the **no** form of this command.

debug mgcp {**messages** | **parser** | **sessions**}

no debug mgcp {**messages** | **parser** | **sessions**}

messages	Displays debug information about MGCP messages.
parser	Displays debug information for parsing MGCP messages.
sessions	Displays debug information about MGCP sessions.

Defaults

All options are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **debug mgcp** command displays detailed information about mgcp inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables the display of detailed information about MGCP application inspection:

```
hostname# debug mgcp
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays information about MGCP sessions established through the security appliance.
show conn	Displays the connection state for different connection types.

debug mmp

To display inspect MMP events, use the **debug mmp** command in privileged EXEC mode. To stop the display of inspect MMP events, use the **no** form of this command.

debug mmp

no debug mmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **debug mmp** command to display inspect MMP events:

```
hostname# debug mmp
ciscoasa5520-tfw-cuma/admin(config-pmap)# MMP:: received 28 bytes from outside:1
72.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: version OLWP-2.0
MMP status: 0
MMP:: forward 28/28 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: version OLWP-2.0
MMP:: session-id: 41A3D410-8B10-4DEB-B15C-B2B4B0D22055
MMP status: 201
MMP:: forward 85/85 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 196
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 200/196
MMP:: forward 265/265 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 198
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 202/198
MMP:: forward 267/267 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 67
```

```
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 71/67
MMP:: forward 135/135 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: content-length: 32
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 36/32
MMP:: forward 100/100 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2442
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: received 220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: content-length: 151
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 155/151
MMP:: forward 220/220 bytes from outside:172.23.62.204/2494 to inside:10.0.0.42/5443
MMP:: received 130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
MMP:: content-length: 62
MMP:: content-type: text/oml21+wbxml
MMP:: processing entity body 66/62
MMP:: forward 130/130 bytes from inside:10.0.0.42/5443 to outside:172.23.62.204/2494
```

Related Commands

Command	Description
inspect mmp	Configures the MMP inspection engine.
show debug mmp	Displays the current debug settings for the MMP inspection module.
show mmp	Displays information about existing MMP sessions.

debug module-boot

To show debug messages about the SSM booting process, use the **debug module-boot** command in privileged EXEC mode. To stop showing debug messages for the SSM booting process, use the **no** form of this command.

debug module-boot [*level*]

no debug module-boot [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for the SSM booting process:

```
hostname# debug module-boot
```

Related Commands

Command	Description
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.

Command	Description
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

debug mrib

To display MRIB debug information, use the **debug mrib** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

debug mrib {**client** | **io** | **route** [*group*] | **table**}

no debug mrib {**client** | **io** | **route** [*group*] | **table**}

Syntax Description

client	Enables debugging for MRIB client management activity.
io	Enables debugging of MRIB I/O events.
route	Enables debugging of MRIB routing entry activity.
group	Enables debugging of MRIB routing entry activity for the specified group.
table	Enables debugging of MRIB table management activity.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows how to enable debugging of MRIB I/O events:

```
hostname# debug mrib io
IPv4 MRIB io debugging is on
```

Related Commands

Command	Description
show mrib client	Displays information about the MRIB client connections.
show mrib route	Displays MRIB table entries.

debug nac

To enable logging of NAC Framework events, use the **debug nac** command in privileged EXEC mode. To disable the logging of NAC debug messages, use the **no** form of this command.

debug nac {**all | auth | errors** | **events**}

no debug nac {**all | auth | errors** | **events**}

Syntax Description

all	Enables logging of debug messages about all NAC information.
auth	Enables logging of debug messages about NAC authentication requests and responses.
errors	Enables logging of NAC session errors.
events	Enables logging of NAC session events.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the security appliance logs the following types of NAC events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the logging of all NAC session events:

```
hostname# debug nac events
hostname#
```

The following example enables the logging of all NAC debug messages:

```
hostname# debug nac all
hostname#
```

The following example disables the logging of all NAC debug messages:

```
hostname# no debug nac
hostname#
```

Related Commands

Command	Description
`debug eap`	Enables logging of Extensible Authentication Protocol events to debug NAC Framework messaging.
`debug eou`	Enables logging of EAP over UDP events to debug NAC Framework messaging.
`show vpn-session_summary.db`	Displays the number of IPSec, WebVPN, and NAC sessions.
`show vpn-session.db`	Displays information about VPN sessions, including NAC results.

debug ntdomain

To display NT domain authentication debug information, use the **debug ntdomain** command in privileged EXEC mode. To disable the display of NT domain debug information, use the **no** form of this command.

debug ntdomain [*level*]

no debug ntdomain

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables NT domain debug messages. The **show debug** command reveals that NT domain debug messages are enabled.

```
hostname# debug ntdomain
debug ntdomain  enabled at level 1
hostname# show debug
debug ntdomain  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug ntp

To show debug messages for NTP, use the **debug ntp** command in privileged EXEC mode. To stop showing debug messages for NTP, use the **no** form of this command.

debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

no debug ntp {**adjust** | **authentication** | **events** | **loopfilter** | **packets** | **params** | **select** | **sync** | **validity**}

Syntax Description

adjust	Shows messages about NTP clock adjustments.
authentication	Shows messages about NTP authentication.
events	Shows messages about NTP events.
loopfilter	Shows messages about NTP loop filter.
packets	Shows messages about NTP packets.
params	Shows messages about NTP clock parameters.
select	Shows messages about NTP clock selection.
sync	Shows messages about NTP clock synchronization.
validity	Shows messages about NTP peer clock validity.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for NTP:

```
hostname# debug ntp events
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp server	Identifies an NTP server.
show debug	Shows all enabled debuggers.
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

debug ospf

To display debug information about the OSPF routing processes, use the **debug ospf** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** [**external** | **inter** | **intra**] | **tree**]

no debug ospf [**adj** | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **spf** [**external** | **inter** | **intra**] | **tree**]

Syntax Description

adj	(Optional) Enables the debugging of OSPF adjacency events.
database-timer	(Optional) Enables the debugging of OSPF timer events.
events	(Optional) Enables the debugging of OSPF events.
external	(Optional) Limits SPF debugging to external events.
flood	(Optional) Enables the debugging of OSPF flooding.
inter	(Optional) Limits SPF debugging to inter-area events.
intra	(Optional) Limits SPF debugging to intra-area events.
lsa-generation	(Optional) Enables the debugging of OSPF summary LSA generation.
packet	(Optional) Enables the debugging of received OSPF packets.
retransmission	(Optional) Enables the debugging of OSPF retransmission events.
spf	(Optional) Enables the debugging of OSPF shortest path first calculations. You can limit the SPF debug information by using the **external**, **inter**, and **intra** keywords.
tree	(Optional) Enables the debugging of OSPF database events.

Defaults

Displays all OSPF debug information if no keyword is provided.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ospf events** command:

```
hostname# debug ospf events
ospf event debugging is on

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

Related Commands

Command	Description
show ospf	Displays general information about the OSPF routing process.

debug parser cache

To display CLI parser debug information, use the **debug parser cache** command in privileged EXEC mode. To disable the display of CLI parser debug information, use the **no** form of this command.

debug parser cache [*level*]

no debug parser cache

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages appear before and after the output of the **show debug** command.

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
parser cache: hit at index 8
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug phone-proxy

To show debug messages for the Phone Proxy instance, use the **debug phone-proxy** command in privileged EXEC mode. To stop displaying Phone Proxy messages, use the **no** form of this command.

debug phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

no debug phone-proxy [<**media** | **signaling** | **tftp**> [**errors** | **events**]]

Syntax Description

errors	(Optional) Show debug messages of phone-proxy errors.
events	(Optional) Show debug messages of phone-proxy events.
media	(Optional) Show debug messages of media sessions for SIP and Skinny inspections.
signaling	(Optional) Show debug messages of signaling sessions for SIP and Skinny inspections.
tftp	(Optional) Show debug messages of TFTP inspection, including creation of the CTL file and configuration file parsing.

Defaults

If no options are specified with the **debug phone-proxy** command, all phone-proxy debugging messages are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The **debug phone-proxy** command displays detailed information about Phone Proxy activity. The **no debug phone-proxy** commands turn off all enabled debugs.

Examples

The following example shows the use of the **debug phone-proxy** command to show successful TFTP transactions for the configuration file request for the Phone Proxy:

```
hostname(config)# debug phone-proxy tftp
PP: 98.208.49.30/1028 requesting SEP00070E364804.cnf.xml.sgn
PP: opened 0x33952aa2
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
        Received Block 1
```

```
PP: Acked Block #1 from 98.208.49.30/1028 to 192.168.200.101/39514
           .... [snip].....
PP: Received data from 192.168.200.101 to outside:98.208.49.30/1028
        Received Block 10
PP: Acked Block #10 from 98.208.49.30/1028 to 192.168.200.101/39514
PP: Installed application redirect rule from 98.208.49.30 to 192.168.200.101 using
redirect port 2000 and secure port 2443
PP: Modifying to TLS as the transport layer protocol.
PP: Modifying to encrypted mode.
PP: Data Block 1 forwarded from 192.168.200.101/39514 to 98.208.49.30/1028
PP: Received ACK Block 1 from outside:98.208.49.30/1028 to inside:192.168.200.101
           ..... [snip] ....
PP: Data Block 11 forwarded to 98.208.49.30/1028
PP: Received ACK Block 11 from outside:98.208.49.30/1028 to inside:192.168.200.101
PP: TFTP session complete, all data sent
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
show running-config phone-proxy	Displays Phone Proxy specific information.

debug pim

To display PI M debug information, use the **debug pim** command in privileged EXEC mode. To stop displaying debug information, use the **no** form of this command.

debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

no debug pim [**df-election** [**interface** *if_name* | **rp** *rp*] | **group** *group* | **interface** *if_name* | **neighbor**]

Syntax Description

df-election	(Optional) Displays debug messages for PIM bidirectional DF-election message processing.
group *group*	(Optional) Displays debug information for the specified group. The value for *group* can be one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
interface *if_name*	(Optional) When used with the **df-election** keyword, it limits the DF election debug display to information for the specified interface. When used without the **df-election** keyword, displays PIM error messages for the specified interface. **Note** The **debug pim interface** command does not display PIM protocol activity messages; it only displays error messages. To see debug information for PIM protocol activity, use the **debug pim** command without the **interface** keyword. You can use the **group** keyword to limit the display to the specified multicast group.
neighbor	(Optional) Displays only the sent/received PIM hello messages.
rp *rp*	(Optional) Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Logs PIM packets received and transmitted and also PIM-related events.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug pim** command:

```
hostname# debug pim
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.6
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16
PIM: Send Prune on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.24.84.16/28
PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Ethernet1)
```

Related Commands

Command	Description
show pim group-map	Displays group-to-protocol mapping table.
show pim interface	Displays interface-specific information for PIM.
show pim neighbor	Displays entries in the PIM neighbor table.

debug pix acl

To show pix acl debug messages, use the **debug pix acl** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix acl

no debug pix acl

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debug messages that :

```
hostname# debug pix acl
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix cls

To show pix cls debug messages, use the **debug pix cls** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix cls

no debug pix cls

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debug messages that :

```
hostname# debug pix cls
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix pkt2pc

To show debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path, use the **debug pix pkt2pc** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix pkt2pc

no debug pix pkt2pc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path:

```
hostname# debug pix pkt2pc
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pix process

To show debug messages for xlate and secondary connections processing, use the **debug pix process** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix process

no debug pix process

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for xlate and secondary connections processing:

```
hostname# debug pix process
```

Related Commands

Command	Description
debug pix pkt2pc	Shows debug messages that trace packets sent to the uauth code and that trace the event where the uauth proxy session is cut through to the data path.
show debug	Shows all enabled debuggers.

debug pix uauth

To showpix uauth debug messages, use the **debug pix uauth** command in privileged EXEC mode. To stop showing debug messages, use the **no** form of this command.

debug pix uauth

no debug pix uauth

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

The following example enables debug messages that :

```
hostname# debug pix uauth
```

Related Commands

Command	Description
debug pix process	Shows debug messages for xlate and secondary connections processing.
show debug	Shows all enabled debuggers.

debug pptp

To show debug messages for PPTP, use the **debug pptp** command in privileged EXEC mode. To stop showing debug messages for PPTP, use the **no** form of this command.

debug pptp [*level*]

no debug pptp [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug pptp** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for PPTP application inspection:

```
hostname# debug pptp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect pptp	Enables PPTP application inspection.

Command	Description
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug radius

To show debug messages for AAA, use the **debug radius** command in privileged EXEC mode. To stop showing RADIUS messages, use the **no** form of this command.

debug radius [**all** | **decode** | **session** | **user** *username*]]

no debug radius

Syntax Description

all	(Optional) Show RADIUS debugging messages for all users and sessions, including decoded RADIUS messages.
decode	(Optional) Show decoded content of RADIUS messages. Content of all RADIUS packets display, including hexadecimal values and the decoded, eye-readable versions of these values.
session	(Optional) Show session-related RADIUS messages. Packet types for sent and received RADIUS messages display but not the packet content.
user	(Optional) Show RADIUS debugging messages for a specific user.
username	Specifies the user whose messages you want to see. Valid with the **user** keyword only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **debug radius** command displays detailed information about RADIUS messaging between the security appliance and a RADIUS AAA server. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example shows decoded RADIUS messages, which happen to be accounting packets:

```
hostname(config)# debug radius decode
hostname(config)# RADIUS packet decode (accounting request)

-------------------------------------
```

```
Raw packet data (length = 216).....
i
Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30 78 31 33 30 31 32 39 66 65                       |  0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72                                |  browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e     |  ip:source-ip=10.
31 2e 31 2e 31 30                                   |  1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 70 6f 72 74 3d 33     |  ip:source-port=3
34 31 33                                            |  413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69     |  ip:destination-i
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35     |  p=10.2.0.50
Radius: Type = 26 (0x1A) Vendor-Specific
```

```
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70    |  ip:destination-p
6f 72 74 3d 38 30                                  |  ort=80
```

Related Commands

Command	Description
show running-config	Displays the configuration that is running on the security appliance.

debug redundant-interface

To show debug messages about redundant interfaces, use the **debug redundant-interface** command in privileged EXEC mode. To stop showing debug messages for redundant interfaces, use the **no** form of this command.

debug redundant-interface [*level*]

no debug redundant-interfac [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for redundant interfaces:

```
hostname# debug redundant-interface
```

Related Commands

Command	Description
interface redundant	Creates a redundant interface.
member-interface	Assigns a physical interface to a redundant interface.
redundant-interface	Changes the active interface in a redundant interface pair.
show debug	Shows all enabled debuggers.

debug rip

To display debug information for RIP, use the **debug rip** command in privileged EXEC mode. To disable the debug information display, use the **no** form of this command.

debug rip [**database** | **events**]

no debug rip [**database** | **events**]

Syntax Description

database	Displays RIP database events.
events	Displays RIP processing events.

Defaults

All RIP events are shown in the debug output.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	The **database** and **events** keywords were added.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug rip** command:

```
hostname# debug rip

RIP: broadcasting general request on GigabitEthernet0/1
RIP: broadcasting general request on GigabitEthernet0/2
RIP: Received update from 10.89.80.28 on GigabitEthernet0/1
    10.89.95.0 in 1 hops
    10.89.81.0 in 1 hops
    10.89.66.0 in 2 hops
    172.31.0.0 in 16 hops (inaccessible)
    0.0.0.0 in 7 hops
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/1 (10.89.64.31)
```

```
    subnet 10.89.94.0, metric 1
    172.31.0.0 in 16 hops (inaccessible)
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/2 (10.89.94.31)
    subnet 10.89.64.0, metric 1
    subnet 10.89.66.0, metric 3
    172.31.0.0 in 16 hops (inaccessible)
    default 0.0.0.0, metric 8
RIP: bad version 128 from 192.168.80.43
```

Related Commands

Command	Description
router rip	Configures a RIP process.
show running-config rip	Displays the RIP commands in the running configuration.

debug rtp

To display debug information and error messages for RTP packets associated with H.323 and SIP inspection, use the **debug rtp** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug rtp [*level*]

no debug rtp [*level*]

Syntax Description

level	(Optional) Specifies an optional level of debug.

Defaults

The default *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example shows how to enable debugging for RTP packets using the **debug rtp** command:

```
hostname# debug rtp 255
debug rtp  enabled at level 255
```

Related Commands

Command	Description
policy-map	Creates a Layer 3/4 policy map.

Command	Description
rtp-conformance	Checks RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP.
show running-config policy-map	Displays all current policy map configurations.

debug rtsp

To show debug messages for RTSP application inspection, use the **debug rtsp** command in privileged EXEC mode. To stop showing debug messages for RTSP application inspection, use the **no** form of this command.

debug rtsp [*level*]

no debug rtsp [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug rtsp** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for RTSP application inspection:

```
hostname# debug rtsp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect rtsp	Enables RTSP application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug sdi

To display SDI authentication debug information, use the **debug sdi** command in privileged EXEC mode. To disable the display of SDI debug information, use the **no** form of this command.

debug sdi [*level*]

no debug sdi

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables SDI debug messages. The **show debug** command reveals that SDI debug messages are enabled.

```
hostname# debug sdi
debug sdi  enabled at level 1
hostname# show debug
debug sdi  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug sequence

To add a sequence number to the beginning of all debug messages, use the **debug sequence** command in privileged EXEC mode. To disable the use of debug sequence numbers, use the **no** form of this command.

debug sequence [*level*]

no debug sequence

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The defaults are as follows:

- Debug message sequence numbers are disabled.
- The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables sequence numbers in debug messages. The **debug parser cache** command enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages shown include sequence numbers before each message.

```
hostname# debug sequence
debug sequence  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
```

```
hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence  enabled at level 1
1: parser cache: hit at index 8
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug session-command

To show debug messages for a session to an SSM, use the **debug session-command** command in privileged EXEC mode. To stop showing debug messages for sessions, use the **no** form of this command.

debug session-command [*level*]

no debug session-command [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for sessions:

```
hostname# debug session-command
```

Related Commands

Command	Description
session	Sessions to an SSM.

debug sip

To show debug messages for SIP application inspection, use the **debug sip** command in privileged EXEC mode. To stop showing debug messages for SIP application inspection, use the **no** form of this command.

debug sip [**ha**]

no debug sip [**ha**]

Syntax Description

ha	(Optional) Display SIP Stateful Failover messages. When this keyword is used with the **debug sip** command on the active unit, debug messages are displayed when SIP state information is sent to the standby unit. When this keyword is used with the **debug sip** command on the standby unit, debug messages are displayed with state updates are received from the active unit.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.
8.0(2)	The **ha** keyword was added.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug sip** command run on the active unit or failover group in a failover pair:

```
hostname# debug sip ha
SIP HA:    Sending    update SESSION message from faddr 10.132.80.120/5060 laddr
10.130.80.4/50295 Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:
State:1

SIP HA:    msg sent to peer successful  Version: 1 Action: update Object: session

SIP HA:    Sending    update TX message from faddr 10.132.80.120/5060laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

The following is sample output from the **debug sip** command run on the standby unit or failover group in a failover pair:

```
hostname# debug sip ha
SIP HA:    Message    received from peer, Version: 1 Action: add Object: session

SIP HA:    Created    SIP session for faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120: 1
total

SIP HA:    Message    received from peer, Version: 1 Action: add Object: tx

SIP HA:    Found an existing session faddr 10.132.80.120/5060 laddr 10.130.80.4/50295
Call-id: 001201e8-8a36000d-196df7f1-17cfef14@10.130.80.4 From:
sip:1004@10.132.80.120:001201e88a3600124a7fad61-640406c0 To: sip:1009@10.132.80.120:

SIP HA:    Created    SIP Transaction    for faddr 10.132.80.120/5060 to   laddr
10.130.80.4/50295CSeq 101 INVITEState Transaction Calling
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sip	Enables SIP application inspection.
show conn	Displays the connection state for different connection types.
show sip	Displays information about SIP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug skinny

To show debug messages for SCCP (Skinny) application inspection, use the **debug skinny** command in privileged EXEC mode. To stop showing debug messages for SCCP application inspection, use the **no** form of this command.

debug skinny [*level*]

no debug skinny [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug skinny** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for SCCP application inspection:

```
hostname# debug skinny
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect skinny	Enables SCCP application inspection.
show skinny	Displays information about SCCP sessions established through the security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug sla monitor

To display debug messages for the SLA monitor operation, use the **debug sla monitor** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sla monitor [**error** | **trace**] [*sla-id*]

no debug sla monitor [*sla-id*]

Syntax Description

error	(Optional) Output IP SLA Monitor Error Messages.
sla-id	(Optional) The ID of the SLA to debug.
trace	(Optional) Output IP SLA Monitor Trace Messages.

Defaults

Both error and trace messages are shown by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Only 32 SLA operations can be debugged at one time.

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables SLA operation error debugging:

```
hostname(config)# debug sla monitor error
```

The following example shows how to display SLA operation trace messages for the specified SLA operation:

```
hostname(config)# debug sla monitor trace 123
```

Related Commands

Command	Description
clear configure route	Removes statically configured **route** commands.
clear route	Removes routes learned through dynamic routing protocols such as RIP.
show route	Displays route information.
show running-config route	Displays configured routes.

debug sqlnet

To show debug messages for SQL*Net application inspection, use the **debug sqlnet** command in privileged EXEC mode. To stop showing debug messages for SQL*Net application inspection, use the **no** form of this command.

debug sqlnet [*level*]

no debug sqlnet [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug sqlnet** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for SQL*Net application inspection:

```
hostname# debug sqlnet
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sqlnet	Enables SQL*Net application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*Net.

debug ssh

To display debug information and error messages associated with SSH, use the **debug ssh** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug ssh [*level*]

no debug ssh [*level*]

Syntax Description

level	(Optional) Specifies an optional level of debug.

Defaults

The default *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug ssh 255** command:

```
hostname# debug ssh 255
debug ssh  enabled at level 255
SSH2 0: send: len 64 (includes padlen 17)
SSH2 0: done calc MAC out #239
SSH2 0: send: len 32 (includes padlen 7)
SSH2 0: done calc MAC out #240
SSH2 0: send: len 64 (includes padlen 15)
SSH2 0: done calc MAC out #241
SSH2 0: send: len 32 (includes padlen 16)
SSH2 0: done calc MAC out #242
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #243
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #244
```

```
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #245
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #246
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #247
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #248
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #249
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #250
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #251
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #252
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #253
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #254
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #255
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #256
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #257
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #258
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.
show ssh sessions	Displays information about active SSH sessions to the security appliance.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.

debug sunrpc

To show debug messages for RPC application inspection, use the **debug sunrpc** command in privileged EXEC mode. To stop showing debug messages for RPC application inspection, use the **no** form of this command.

debug sunrpc [*level*]

no debug sunrpc [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug sunrpc** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for RPC application inspection:

```
hostname# debug sunrpc
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sunrpc	Enables Sun RPC application inspection.
policy-map	Associates a class map with specific security actions.
show conn	Displays the connection state for different connection types, including RPC.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug switch ilpm

To show debug messages for models with a built-in switch, such as the ASA 5505 adaptive security appliance, show debug messages for PoE, use the **debug switch ilpm** command in privileged EXEC mode. To stop showing debug messages for PoE, use the **no** form of this command.

debug switch ilpm [**events** | **errors**] [*level*]

no debug switch ilpm [**events** | **errors**] [*level*]

Syntax Description

errors	(Optional) Shows troubleshooting information when there is an error.
events	(Optional) Shows PoE events.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

By default, both events and errors are shown if you do not specify a keyword. The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for PoE ports:

```
hostname# debug switch ilpm
```

Related Commands

Command	Description
interface vlan	Adds a VLAN interface.
debug switch manager	Shows debug messages for VLAN assignment and **switchport** command-caused events and errors.
show debug	Shows all enabled debuggers.

debug switch manager

To show debug messages for switch port models with a built-in switch, such as the ASA 5505 adaptive security appliance, show debug messages for VLAN assignment, and **switchport** command-caused events and errors, use the **debug switch manager** command in privileged EXEC mode. To stop showing debug messages for switch ports, use the **no** form of this command.

debug switch manager [**events** | **errors**] [*level*]

no debug switch manager [**events** | **errors**] [*level*]

Syntax Description

errors	(Optional) Shows troubleshooting information when there is an error.
events	(Optional) Shows the switch manager events.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

By default, both events and errors are shown if you do not specify a keyword. The default level is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Using **debug** commands might slow down traffic on busy networks.

Examples

The following example enables debug messages for switch ports:

```
hostname# debug switch manager
```

Related Commands

Command	Description
interface vlan	Adds a VLAN interface.
debug switch ilpm	Shows debug messages for PoE.
show debug	Shows all enabled debuggers.

debug tacacs

To display TACACS+ debug information, use the **debug tacacs** command in privileged EXEC mode. To disable the display of TACACS+ debug information, use the **no** form of this command.

debug tacacs [**session** | **user** *username*]

no debug tacacs [**session** | **user** *username*]

Syntax Description

session	Displays session-related TACACS+ debug messages.
user	Displays user-specific TACACS+ debug messages. You can display TACACS+ debug messages for only one user at a time.
username	Specifies the user whose TACACS+ debug messages you want to view.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables TACACS+ debug messages. The **show debug** command reveals that TACACS+ debug messages are enabled.

```
hostname# debug tacacs user admin342
hostname# show debug
debug tacacs user admin342
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug tcp-map

To show debug messages for TCP application inspection maps, use the **debug tcp-map** command in privileged EXEC mode. To stop showing debug messages for TCP application inspection, use the **no** form of this command.

debug tcp-map

no debug tcp-map

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables debug messages for TCP application inspection maps. The **show debug** command reveals that debug messages for TCP application inspection maps are enabled.

```
hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug timestamps

To add timestamp information to the beginning of all debug messages, use the **debug timestamps** command in privileged EXEC mode. To disable the use of debug timestamps, use the **no** form of this command.

debug timestamps [*level*]

no debug timestamps

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The defaults are as follows:

- Debug timestamp information is disabled.
- The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables timestamps in debug messages. The **debug parser cache** command enables CLI parser debug messages. The **show debug** command reveals the current debug configuration. The CLI parser debug messages shown include timestamps before each message.

```
hostname# debug timestamps
debug timestamps  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
```

```
hostname# show debug
1982769.770000000: parser cache: try to match 'show debug' in exec mode
1982769.770000000: parser cache: hit at index 8
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug vpn-sessiondb

To display VPN-session database debug information, use the **debug vpn-sessiondb** command in privileged EXEC mode. To disable the display of VPN-session database debug information, use the **no** form of this command.

debug vpn-sessiondb [*level*]

no debug vpn-sessiondb

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables VPN-session database debug messages. The **show debug** command reveals that VPN-session database debug messages are enabled.

```
hostname# debug vpn-sessiondb
debug vpn-sessiondb  enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug wccp

To enable logging of WCCP events, use the **debug wccp** command in privileged EXEC mode. To disable the logging of WCCP debug messages, use the **no** form of this command.

debug wccp {**events | packets | subblocks**}

no debug wccp {**events | packets | subblocks**}

Syntax Description

events	Enables logging of WCCP session events.
packets	Enables logging of debug messages about WCCP packet information.
subblocks	Enables logging of debug messages about WCCP subblocks.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables the logging of all WCCP session events:

```
hostname# debug wccp events
hostname#
```

The following example enables the logging of WCCP packet debug messages:

```
hostname# debug wccp packets
hostname#
```

The following example disables the logging of WCCP debug messages:

```
hostname# no debug wccp
```

```
hostname#
```

Related Commands

Command	Description
wccp	Enables support of WCCP.
show debug	Displays current debug configuration.

debug webvpn

To log WebVPN debug messages, use the **debug webvpn** command in privileged EXEC mode. To disable the logging of WebVPN debug messages, use the **no** form of this command.

debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

no debug webvpn [**chunk** | **cifs** | **citrix** | **failover** | **html** | **javascript** | **request** | **response** | **svc** | **transformation** | **url** | **util** | **xml**] [*level*]

Syntax Description

chunk	Displays debug messages about memory blocks used to support WebVPN connections.
cifs	Displays debug messages about connections between CIFS)servers and WebVPN users.
citrix	Displays debug messages about connections between Citrix Metaframe Servers and Citrix ICA clients over WebVPN.
failover	Displays debug messages about equipment failovers affecting WebVPN connections.
html	Displays debug messages about HTML pages sent over WebVPN connections.
javascript	Displays debug messages about JavaScript sent over WebVPN connections.
request	Displays debug messages about requests issued over WebVPN connections.
response	Displays debug messages about responses issued over WebVPN connections.
svc	Displays debug messages about connections to SSL VPN clients over WebVPN.
transformation	Displays debug messages about WebVPN content transformation.
url	Displays debug messages about website requests issued over WebVPN connections.
util	Displays debug messages about CPU utilization dedicated to support connections to WebVPN remote users.
xml	Displays debug messages about JavaScript sent over WebVPN connections.
level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The high priority assigned to debugging output can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following example enables WebVPN debug messages, specifically for CIFS. The **show debug** command reveals that CIFS debug messages are enabled.

```
hostname# debug webvpn cifs
INFO: debug webvpn cifs enabled at level 1.
hostname# show debug
debug webvpn cifs enabled at level 1
hostname#
```

Related Commands

Command	Description
show debug	Displays current debug configuration.

debug xdmcp

To show debug messages for XDMCP application inspection, use the **debug xdmcp** command in privileged EXEC mode. To stop showing debug messages for XDMCP application inspection, use the **no** form of this command.

debug xdmcp [*level*]

no debug xdmcp [*level*]

Syntax Description

level	(Optional) Sets the debug message level to display, between 1 and 255. The default is 1. To display additional messages at higher levels, set the level to a higher number.

Defaults

The default value for *level* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To see the current debug command settings, enter the **show debug** command. To stop the debug output, enter the **no debug** command. To stop all debug messages from being displayed, enter the **no debug all** command.

Note Enabling the **debug xdmcp** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for XDMCP application inspection:

```
hostname# debug xdmcp
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect xdmcp	Enables XDMCP application inspection.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

debug xml

To display debug information for the XML parser, use the **debug xml** command in privileged EXEC mode. To disable the display of debug information, use the **no** form of this command.

debug xml [**element** | **event**]

no debug xml [**element** | **event**]

Syntax Description

element	(Optional) Displays debug events related to processing individual XML elements.
event	(Optional) Displays XML parsing or error events.

Defaults

If no keywords are specified, all XML parser debug messages are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The following is sample output from the **debug xml element** command:

```
hostname# debug xml element
debug xml element enabled at level 1

XML Executes cmd: hostname hostname
XML Executes cmd: domain-name example.com
XML Executes cmd: names
XML Executes cmd: dns-guard
XML Executes cmd: !
XML Executes cmd: interface Ethernet0
XML Executes cmd:  nameif outside
XML Executes cmd:  security-level 0
```

```
XML Executes cmd:  ip address 192.168.5.151 255.255.255.0 standby 192.168.5.152
XML Executes cmd: interface Ethernet1
XML Executes cmd:  nameif inside
XML Executes cmd:  security-level 100
XML Executes cmd:  ip address 192.168.0.151 255.255.255.0 standby 192.168.0.152
XML Executes cmd: !
XML Executes cmd: boot system flash:/f
XML Executes cmd: ftp mode passive
XML Executes cmd: clock timezone jst 9
XML Executes cmd: dns server-group DefaultDNS
XML Executes cmd:  domain-name cisco.com
_tcp_listen: could not query index for interface 65535 port 23
XML Executes cmd: pager lines 24
XML Executes cmd: logging console debugging
XML Executes cmd: logging buffered debugging
XML Executes cmd: mtu outside 1500
XML Executes cmd: mtu inside 1500
XML Executes cmd: failover
XML Executes cmd: no asdm history enable
XML Executes cmd: arp timeout 14000
XML Executes cmd: route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
XML Executes cmd: timeout xlate 3:00:00
XML Executes cmd: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
XML Executes cmd: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
XML Executes cmd: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
XML Executes cmd: timeout uauth 0:05:00 absolute
XML Executes cmd: username user1 password mbO2jYs13AXlIAGa encrypted
XML Executes cmd: username sugi password EB3OP7Hu2hSu6x/7 encrypted
XML Executes cmd: http server enable
XML Executes cmd: http 0.0.0.0 0.0.0.0 outside
XML Executes cmd: no snmp-server location
XML Executes cmd: no snmp-server contact
XML Executes cmd: snmp-server enable traps snmp authentication linkup linkdown coldstart
XML Executes cmd: telnet timeout 5
XML Executes cmd: ssh timeout 5
XML Executes cmd: console timeout 0
XML Executes cmd: !
XML Executes cmd: class-map inspection_default
XML Executes cmd:  match default-inspection-traffic
XML Executes cmd: !
XML Executes cmd: !
XML Executes cmd: policy-map type inspect dns migrated_dns_map_1
XML Executes cmd:  parameters
XML Executes cmd:   message-length maximum 512
XML Executes cmd: policy-map global_policy
XML Executes cmd:  class inspection_default
XML Executes cmd:   inspect ftp
XML Executes cmd:   inspect h323 h225
XML Executes cmd:   inspect h323 ras
XML Executes cmd:   inspect netbios
XML Executes cmd:   inspect rsh
XML Executes cmd:   inspect rtsp
XML Executes cmd:   inspect skinny
XML Executes cmd:   inspect esmtp
XML Executes cmd:   inspect sqlnet
XML Executes cmd:   inspect sunrpc
XML Executes cmd:   inspect tftp
XML Executes cmd:   inspect sip
XML Executes cmd:   inspect xdmcp
XML Executes cmd: !
XML Executes cmd: service-policy global_policy global
XML error info: cmd-id 87 type info
```

```
XML Executes cmd: prompt hostname context
XML Executes cmd: crashinfo save disable
```

The following is sample output from the **debug xml event** command:

```
hostname# debug xml event
debug xml event enabled at level 1

XML parsing: data = <con... len = 3176
Exit XML parser, ret code = 0
```

Related Commands

Command	Description
show debug	Displays the debugging status for the various **debug** commands.

CHAPTER 11

default (crl configure) through dynamic-access-policy-record Commands

default (crl configure)

To return all CRL parameters to their system default values, use the **default** command in crl configure configuration mode. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

default

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•		•		

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the active configuration.

Examples

The following example enters ca-crl configuration mode, and returns CRL command values to their defaults:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configure configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

default (interface)

To return an interface command to its system default value, use the **default** command in interface configuration mode.

default *command*

Syntax Description

command	Specifies the command that you want to set to the default. For example: `default activation key`

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is a run-time command; when you enter it, it does not become part of the active configuration.

Examples

The following example enters interface configuration mode, and returns the security level to its default:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# default security-level
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

default (time-range)

To restore default settings for the **absolute** and **periodic** commands, use the **default** command in time-range configuration mode.

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

Syntax Description

absolute	Defines an absolute time when a time range is in effect.
days-of-the-week	The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Defaults

There are no default settings for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Time-range configuration	•	•	•	•	

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.

Examples

The following example shows how to restore the default behavior of the **absolute** keyword:

```
hostname(config-time-range)# default absolute
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the security appliance based on time.

default-acl

To specify the ACL to be used as the default ACL for NAC Framework sessions that fail posture validation, use the **default-acl** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of the command.

[no] **default-acl** *acl-name*

Syntax Description

acl-name	Names the access control list to be applied to the session.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	"nac-" removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

Each group policy points to a default ACL to be applied to hosts that match the policy and are eligible for NAC. The security appliance applies the NAC default ACL before posture validation. Following posture validation, the security appliance replaces the default ACL with the one obtained from the Access Control Server for the remote host. It retains the default ACL if posture validation fails.

The security appliance also applies the NAC default ACL if clientless authentication is enabled (which is the default setting).

Examples

The following example identifies acl-1 as the ACL to be applied before posture validation succeeds:

```
hostname(config-group-policy)# default-acl acl-1
hostname(config-group-policy)
```

The following example inherits the ACL from the default group policy.

```
hostname(config-group-policy)# no default-acl
hostname(config-group-policy)
```

Related Commands

Command	Description
`nac-policy`	Creates and accesses a Cisco NAC policy, and specifies its type.
`nac-settings`	Assigns a NAC policy to a group policy.
`debug nac`	Enables logging of NAC Framework events
`show vpn-session_summary.db`	Displays the number IPSec, WebVPN, and NAC sessions.
`show vpn-session.db`	Displays information about VPN sessions, including NAC results.

default enrollment

To return all enrollment parameters to their system default values, use the **default enrollment** command in crypto ca trustpoint configuration mode.

default enrollment

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the active configuration.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and returns all enrollment parameters to their default values within trustpoint central:

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># default enrollment
hostname<ca-trustpoint>#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

default-domain

To set a default domain name for users of the group policy, use the **default-domain** command in group-policy configuration mode. To delete a domain name, use the **no** form of this command.

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

Syntax Description

none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.
value *domain-name*	Identifies the default domain name for the group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To prevent users from inheriting a domain name, use the **default-domain none** command.

The security appliance passes the default domain name to the IPSec client to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. When there are no default domain names, users inherit the default domain name in the default group policy.

You can use only alphanumeric characters, hyphens (-), and periods (.) in default domain names.

Examples

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

Related Commands

Command	Description
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form.

default-group-policy

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

default-group-policy *group-name*

no default-group-policy *group-name*

Syntax Description

group-name	Specifies the name of the default group.

Defaults

The default group name is DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Version	Modification
7.0(1)	This command was introduced.
7.1(1)	The **default-group-policy** command in webvpn configuration mode was deprecated. The **default-group-policy** command in tunnel-group general-attributes mode replaces it.

Usage Guidelines

In Version 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

The default group policy DfltGrpPolicy comes with the initial configuration of the security appliance. You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-general configuration mode, specifies a set of attributes for users to inherit by default for an IPSec LAN-to-LAN tunnel group named “standard-policy”. This set of commands defines the accounting server, the authentication server, the authorization server and the address pools.

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)# authentication-server-group aaa-server456
```

```
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-policy	Creates or edits a group policy
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

default-group-policy (webvpn)

To specify the name of the group policy to use when the WebVPN or e-mail proxy configuration does not specify a group policy, use the **default-group-policy** command in various configuration modes. To remove the attribute from the configuration, use the **no** version of this command.

default-group-policy *groupname*

no default-group-policy

Syntax Description

groupname	Identifies the previously configured group policy to use as the default group policy. Use the **group-policy** command to configure a group policy.

Defaults

A default group policy, named *DfltGrpPolicy*, always exists on the security appliance. This **default-group-policy** command lets you substitute a group policy that you create as the default group policy for WebVPN and e-mail proxy sessions. An alternative is to edit the DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—
Imap4s configuration	•	—	•	—	—
Pop3s configuration	•	—	•	—	—
Smtps configuration	•	—	•	—	—

Command History

Version	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

WebVPN, IMAP4S, POP3S, and SMTPS sessions require either a specified or a default group policy. For WebVPN, use this command in webvpn mode. For e-mail proxy, use this command in the applicable e-mail proxy mode.

In Version 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

You can edit, but not delete the system DefaultGroupPolicy. It has the following AVPs:

Attribute	Default Value
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn attributes:	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	mpme

Examples

The following example shows how to specify a default group policy called WebVPN7 for WebVPN:

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

To set a default idle timeout value for WebVPN users, use the **default-idle-timeout** command in webvpn configuration mode. To remove the default idle timeout value from the configuration and reset the default, use the **no** form of this command.

The default idle timeout prevents stale sessions.

default-idle-timeout *seconds*

no default-idle-timeout

Syntax Description

seconds	Specifies the number of seconds for the idle time out. The minimum is 60 seconds, maximum is 1 day (86400 seconds).

Defaults

1800 seconds (30 minutes).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The security appliance uses the value you set here if there is no idle timeout defined for a user, if the value is 0, or if the value does not fall into the valid range.

We recommend that you set this command to a short time period. This is because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the maximum number of connections permitted is set to one (**vpn-simultaneous-logins** command), the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.

Examples

The following example shows how to set the default idle timeout to 1200 seconds (20 minutes):

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

Related Commands

Command	Description
vpn-simultaneous-logins	Sets the maximum number of simultaneous VPN sessions permitted. Use in group-policy or username mode.

default-information (EIGRP)

To control the candidate default route information for the EIGRP routing process, use the **default-information** command in router configuration mode. To suppress EIGRP candidate default route information in incoming or outbound updates, use the **no** form of this command.

default-information {**in** | **out**} [*acl-name*]

no default-information {**in** | **out**}

Syntax Description

acl-name	(Optional) Named standard access list.
in	Configures EIGRP to accept exterior default routing information.
out	Configures EIGRP to advertise external routing information.

Defaults

Exterior routes are accepted and sent.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Only the **no** form of the command or **default-information** commands with an access list specified will appear in the running configuration because, by default, the candidate default routing information is accepted and sent. The **no** form of the command does not take an *acl-name* argument.

Examples

The following example disables the receipt of exterior or candidate default route information:

```
hostname(config)# router eigrp 100
hostname(config-router)# no default-information in
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

default-information originate (OSPF)

To generate a default external route into an OSPF routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric *value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type {1 | 2}	(Optional) External link type associated with the default route advertised into the OSPF routing domain. Valid values are as follows: • **1**—Type 1 external route. • **2**—Type 2 external route.
route-map *name*	(Optional) Name of the route map to apply.

Defaults

The default values are as follows:

- **metric** *value* is 1.
- **metric-type** is 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Using the **no** form of this command with optional keywords and arguments only removes the optional information from the command. For example, entering **no default-information originate metric** *3* removes the **metric** *3* option from the command in the running configuration. To remove the complete command from the running configuration, use the **no** form of the command without any options: **no default-information originate**.

Examples

The following example shows how to use the **default-information originate** command with an optional metric and metric type:

```
hostname(config-router)# default-information originate always metric 3 metric-type 2
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

default-information originate (RIP)

To generate a default route into RIP, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]]

Syntax Description

route-map *name*	(Optional) Name of the route map to apply. The routing process generates the default route if the route map is satisfied.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The route map referenced in the **default-information originate** command cannot use an extended access list; it can use a standard access list.

Examples

The following example shows how generate a default route into RIP:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# default-information originate
```

Related Commands

Command	Description
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

default-language

To set the default language displayed on the Clientless SSL VPN pages, use the **default-language** command from webvpn configuration mode.

default-language *language*

Syntax Description

language	Specifies the name of a previously-imported translation table.

Defaults

The default language is en-us (English spoken in the United States).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

The default language is displayed to the Clientless SSL VPN user when they initially connect to the security appliance, before logging in. Thereafter, the language displayed is affected by the tunnel group or group policy settings and any customization that they reference.

Examples

The following example changes the default language to Chinese:with the name *Sales*:

```
hostname(config-webvpn)# default-language zh
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

default-metric

To specify the EIGRP metrics for redistributed routes, use the **default-metric** command in router configuration mode. To restore the default values, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

bandwidth	The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
delay	The route delay in tens of microseconds. Valid values are 1 to 4294967295.
reliability	The likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.
loading	The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
mtu	The smallest allowed value for the MTU, expressed in bytes. Valid values are from 1 to 65535.

Defaults

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP unless you use the **metric** keyword and attributes in the **redistribute** command. Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values. Keeping the same metrics is supported only when you are redistributing from static routes.

Examples

The following example shows how the redistributed RIP route metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 172.16.0.0
hostname(config-router)# redistribute rip
hostname(config-router)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters router configuration mode for that process.
redistribute (EIGRP)	Redistributes routes into the EIGRP routing process.

delay

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

delay *delay-time*

no delay

Syntax Description

delay-time	The delay time in tens of microseconds. Valid values are from 1 to 16777215.

Defaults

The default delay depends upon the interface type. Use the **show interface** command to see the delay value for an interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The value entered is in tens of microseconds. The delay value displayed in the **show interface** output is in microseconds.

Examples

The following example changes the delay on an interface from the default 1000 to 2000. Truncated **show interface** command output is included before and after the **delay** command to show how the command affects the delay values. The delay value is noted in the second line of the **show interface** output, after the DLY label.

Notice that the command entered to change the delay value to 2000 is **delay 200**, not **delay 2000**. This is because the value entered with the **delay** command is in tens of microseconds, and the **show interface** output displays microseconds.

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
```

```
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed

hostname(config-if)# delay 200
hostname(config-if)# show interface Ethernet0/0

Interface Ethernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 100 Mbps, DLY 2000 usec
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 0013.c480.7e16, MTU 1500
        IP address 10.86.194.224, subnet mask 255.255.254.0
! Remainder of the output removed
```

Related Commands

Command	Description
show interface	Displays interface statistics and settings.

delete

To delete a file in the disk partition, use the **delete** command in privileged EXEC mode.

delete [**/noconfirm**] [**/recursive**] [**flash:**]*filename*

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
/recursive	(Optional) Deletes the specified file recursively in all subdirectories.
filename	Specifies the name of the file to delete.
flash:	Specifies the nonremovable internal Flash, followed by a colon.

Defaults

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files. When deleting files, you are prompted with the filename and you must confirm the deletion.

The following example shows how to delete a file named *test.cfg* in the current working directory:

```
hostname# delete test.cfg
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
rmdir	Removes a file or directory.
show file	Displays the specified file.

deny-message (group-policy webvpn configuration mode)

To change the message delivered to a remote user who logs into WebVPN successfully, but has no VPN privileges, use the **deny-message value** command in group-webvpn configuration mode.To remove the string so that the remote user does not receive a message, use the **no** form of this command.

deny-message value "*string*"

no deny-message value

Syntax Description

string	Up to 491 alphanumeric characters, including special characters, spaces, and punctuation.

Defaults

The default deny message is: “Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.”

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command moved from tunnel-group webvpn configuration mode to group-webvpn configuration mode.

Usage Guidelines

Before entering this command, you must enter the **group-policy** *name* **attributes** in global configuration mode, then the **webvpn** command. (This assumes you already have created the policy *name*.)

The **no deny-message none** command removes the attribute from the group-webvp configuration. The policy inherits the attribute value.

When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The text appears on the remote user’s browser upon login, independent of the tunnel policy used for the VPN session.

Examples

The following example shows the first command that creates an internal group policy named group2. The subsequent commands modify the deny message associated with that policy.

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

Related Commands

Command	Description
clear configure group-policy	Removes all group-policy configuration.
group-policy	Creates a group policy.
group-policy attributes	Enters the group-policy attribute configuration mode.
show running-config group-policy [*name*]	Displays the running group policy configuration for the policy named.
webvpn (group-policy or username configuration mode)	Enters group-pollicy webvpn configuration mode.

deny version

To deny a specific version of SNMP traffic, use the **deny version** command in snmp-map configuration mode, which is accessible by entering the **snmp-map** command from global configuration mode. To disable this command, use the **no** form of this command.

deny version *version*

no deny version *version*

Syntax Description

version	Specifies the version of SNMP traffic that the security appliance drops. The permitted values are **1**, **2**, **2c**, and **3**.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Snmp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **deny version** command to restrict SNMP traffic to specific versions of SNMP. Earlier versions of SNMP were less secure, so restricting SNMP traffic to Version 2 may be specified by your security policy. You use the **deny version** command within an SNMP map, which you configure using the **snmp-map** command. After creating the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
```

```
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect snmp	Enable SNMP application inspection.
policy-map	Associates a class map with specific security actions.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
service-policy	Applies a policy map to one or more interfaces.

description

To add a description for a named configuration unit (for example, for a context or for an object group, or for a DAP record), use the **description** command in various configuration modes. The description adds helpful notes in your configuration To remove the description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Sets the description as a text string up to 200 characters in length. For dynamic-access-policy-record mode the maximum length is 80 characters. If you want to include a question mark (?) in the string, you must type **Ctrl-V** before typing the question mark so you do not inadvertently invoke CLI help.

Defaults

No default behavior or values.

Command Modes

This command is available in various configuration modes.

Command History

Release	Modification
Preexisting	This command was preexisting.
8.0(2)	Support added for dynamic-access-policy-record mode.

Examples

The following example adds a description to the “Administration” context configuration:

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://admin.cfg
```

Related Commands

Command	Description
class-map	Identifies traffic to which you apply actions in the **policy-map** command.
context	Creates a security context in the system configuration and enters context configuration mode.
gtp-map	Controls parameters for the GTP inspection engine.
interface	Configures an interface and enters interface configuration mode.
object-group	Identifies traffic to include in the **access-list** command.
policy-map	Identifies actions to apply to traffic identified by the **class-map** command.

dhcp client route distance

To configure an administrative distance for routes learned through DHCP, use the **dhcp client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

dhcp client route distance *distance*

no dhcp client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through DHCP. Valid values are from 1 to 255.

Defaults

Routes learned through DHCP are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **dhcp client route distance** command is checked only when a route is learned from DHCP. If the **dhcp client route distance** command is entered after a route is learned from DHCP, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
```

```
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route track	Associates routes learned through DHCP with a tracking entry object.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp client route track

To configure the DHCP client to associate added routes with a specified tracked object number, use the **dhcp client route track** command in interface configuration mode. To disable DHCP client route tracking, use the **no** form of this command.

dhcp client route track *number*

no dhcp client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **dhcp client route track** command is checked only when a route is learned from DHCP. If the **dhcp client route track** command is entered after a route is learned from DHCP, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route distance	Assigns an administrative distance to routes learned through DHCP.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp-client broadcast-flag

To allow the security appliance to set the broadcast flag in the DHCP client packet, use the **dhcp-client broadcast-flag** command in global configuration mode. To disallow the broadcast flag, use the **no** form of this command.

dhcp-client broadcast-flag

no dhcp-client broadcast-flag

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the broadcast flag is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1.

If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address.

The DHCP client can receive both broadcast and unicast offers from the DHCP server.

Examples

The following example enables the broadcast flag:

```
hostname(config)# dhcp-client broadcast-flag
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.

dhcp-client client-id	Sets DHCP request packet option 61 to include the interface MAC address.
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp-client client-id

To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally-generated string, use the **dhcp-client client-id** command in global configuration mode. To disallow the MAC address, use the **no** form of this command.

dhcp-client client-id interface *interface_name*

no dhcp-client client-id interface *interface_name*

Syntax Description

interface *interface_name*	Specifies the interface on which you want to enable the MAC address for option 61.

Defaults

By default, an internally-generated ASCII string is used for option 61.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use the **dhcp-client client-id** command to include the interface MAC address for option 61.

Examples

The following example enables the MAC address for option 61 for the outside interface:

```
hostname(config)# dhcp-client client-id interface outside
```

Related Commands

Command	Description
ip address dhcp	Enables the DHCP client for an interface.
interface	Enters interface configuration mode so you can set the IP address.

dhcp-client broadcast-flag	Sets the broadcast flag in the DHCP client packet.
dhcp-client update dns	Enables DNS updates for the DHCP client.

dhcp-client update dns

To configure the update parameters that the DHCP client passes to the DHCP server, use the **dhcp-client update dns** command in global configuration mode. To remove the parameters that the DHCP client passes to the DHCP server, use the **no** form of this command.

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

Syntax Description

both	The client requests that the DHCP server update both the DNS A and PTR resource records.
none	The client requests that the DHCP server perform no DDNS updates.
server	Specifies the DHCP server to receive the client requests.

Defaults

By default, the security appliance requests that the DHCP server perform PTR RR updates only. The client does not send the FQDN option to the server.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can also be entered in interface configuration mode, but it is not hyphenated. See **dhcp client update dns**. When entered in interface mode, the **dhcp client update dns** command overrides settings configured by this command in global configuration mode.

Examples

The following example configures the client to request that the DHCP server update neither the A and the PTR RRs:

```
hostname(config)# dhcp-client update dns server none
```

The following example configures the client to request that the server update both the A and PTR RRs:

```
hostname(config)# dhcp-client update dns server both
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp client update dns	
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcp-network-scope

To specify the range of IP addresses the security appliance DHCP server should use to assign addresses to users of this group policy, use the **dhcp-network-scope** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy. To prevent inheriting a value, use the **dhcp-network-scope none** command.

dhcp-network-scope {*ip_address*} | none

no dhcp-network-scope

Syntax Description

ip_address	Specifies the IP subnetwork the DHCP server should use to assign IP addresses to users of this group policy.
none	Sets the DHCP subnetwork to a null value, thereby allowing no IP addresses. Prevents inheriting a value from a default or specified group policy.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set an IP subnetwork of 10.10.85.0 for the group policy named First Group:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

dhcp-server

To configure support for DHCP servers that assign IP addresses to clients as a VPN tunnel is established, use the **dhcp-server** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

[no] dhcp-server [link-selection | subnet-selection] <ip1> [<ip2>...<ip10>]

Syntax Description

<ip1>	Address of a DHCP server
<ip2>-<ip10>	(Optional) Additional DHCP servers Up to ten may be specified in the same command or spread over multiple commands
link-selection	(Optional) Setting to specify that the security appliance should send DHCP sub-option 5, the Link Selection Sub-option for the Relay Information Option 82, defined by RFC 3527. This should only be used with servers that support this RFC.
subnet-selection	(Optional) setting to specify that the security appliance should send DHCP Option 118, the IPv4 Subnet Selection Option, defined by RFC 3011. This should only be used with servers that support this RFC.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(5)	Added the link-selection and subnet-selection options.

Usage Guidelines

You can apply this attribute to IPSec remote access tunnel-group types only.

Examples

The following command entered in config-general configuration mode, adds three DHCP servers (dhcp1, dhcp2, and dhcp3) to the IPSec remote-access tunnel group “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-tunnel-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

dhcpd address

To define the IP address pool used by the DHCP server, use the **dhcpd address** command in global configuration mode. To remove an existing DHCP address pool, use the **no** form of this command.

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

Note The size of the pool is limited to 32 addresses with a 10-user license and 128 addresses with a 50-user license on the Cisco ASA 5505. The unlimited user license on the Cisco ASA 5505 and all other security appliance platforms support 256 addresses.

Syntax Description

interface_name	Interface the address pool is assigned to.
IP_address1	Start address of the DHCP address pool.
IP_address2	End address of the DHCP address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd address** *ip1*[*-ip2*] *interface_name* command specifies the DHCP server address pool. The address pool of a security appliance DHCP server must be within the same subnet of the security appliance interface on which it is enabled, and you must specify the associated security appliance interface using *interface_name*.

The size of the address pool is limited to 256 addresses per pool on the security appliance. If the address pool range is larger than 253 addresses, the netmask of the security appliance interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

DHCP clients must be physically connected to the subnet of the security appliance DCHP server interface.

The **dhcpd address** command cannot use interface names with a "-" (dash) character because the "-" character is interpreted as a range specifier instead of as part of the object name.

The **no dhcpd address** *interface_name* command removes the DHCP server address pool that you configured for the specified interface.

Refer to the *Cisco ASA 5500 Series Configuration Guide using the CLI* for information on how to implement the DHCP server feature into the security appliance.

Examples

The following example shows how to use the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** *interface_name* commands to configure an address pool and DNS server for the DHCP clients on the **dmz** interface of the security appliance:

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

The following example shows how to configure a DHCP server on the inside interface. It uses the **dhcpd address** command to assign a pool of 10 IP addresses to the DHCP server on that interface.

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd auto_config

To enable the security appliance to automatically configure DNS, WINS and domain name values for the DHCP server based on the values obtained from an interface running a DHCP or PPPoE client, or from a vpn server, use the **dhcpd auto_config** command in global configuration mode. To discontinue the automatic configuration of DHCP parameters, use the **no** form of this command.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Syntax Description

client_if_name	Specifies the interface running the DHCP client that supplies the DNS, WINS, and domain name parameters.
interface *if_name*	Specifies the interface to which the action will apply.
vpnclient-wins-override	Overrides interface DHCP or PPPoE client WINS parameter with vpnclient parameter.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you specify DNS, WINS, or domain name parameters using the CLI commands, then the CLI-configured parameters overwrite the parameters obtained by automatic configuration.

Examples

The following example shows how to configure DHCP on the inside interface. The **dhcpd auto_config** command is used to pass DNS, WINS, and domain information obtained from the DHCP client on the outside interface to the DHCP clients on the inside interface.

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd autoconfig outside
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show ip address dhcp server	Displays detailed information about the DHCP options provided by a DHCP server to an interface acting as a DHCP client.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd dns

To define the DNS servers for DHCP clients, use the **dhcpd dns** command in global configuration mode. To clear defined servers, use the **no** form of this command.

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns [*dnsip1* [*dnsip2*]] [**interface** *if_name*]

Syntax Description

dnsip1	IP address of the primary DNS server for the DHCP client.
dnsip2	(Optional) IP address of the alternate DNS server for the DHCP client.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd dns** command lets you specify the IP address or addresses of the DNS server(s) for the DHCP client. You can specify two DNS servers. The **no dhcpd dns** command lets you remove the DNS IP address(es) from the configuration.

Examples

The following example shows how to use the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** *interface_name* commands to configure an address pool and DNS server for the DHCP clients on the **dmz** interface of the security appliance.

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd enable	Enables the DHCP server on the specified interface.
dhcpd wins	Defines the WINS servers for DHCP clients.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd domain

To define the DNS domain name for DHCP clients, use the **dhcpd domain** command in global configuration mode. To clear the DNS domain name, use the **no** form of this command.

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

Syntax Description

domain_name	The DNS domain name, for example example.com.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd domain** command lets you specify the DNS domain name for the DHCP client. The **no dhcpd domain** command lets you remove the DNS domain server from the configuration.

Examples

The following example shows how to use the **dhcpd domain** command to configure the domain name supplied to DHCP clients by the DHCP server on the security appliance:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd enable

To enable the DHCP server, use the **dhcpd enable** command in global configuration mode. To disable the DHCP server, use the **no** form of this command. The DHCP server provides network configuration parameters to DHCP clients. Support for the DHCP server within the security appliance means that the security appliance can use DHCP to configure connected clients.

dhcpd enable *interface*

no dhcpd enable *interface*

Syntax Description

interface	Specifies the interface on which to enable the DHCP server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd enable** *interface* command lets you enable the DHCP daemon to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.

Note For multiple context mode, you cannot enable the DHCP server on an interface that is used by more than one context (a shared VLAN).

When the security appliance responds to a DHCP client request, it uses the IP address and subnet mask of the interface where the request was received as the IP address and subnet mask of the default gateway in the response.

Note The security appliance DHCP server daemon does not support clients that are not directly connected to a security appliance interface.

Refer to the *Cisco ASA 5500 Series Configuration Guide using the CLI* for information on how to implement the DHCP server feature into the security appliance.

Examples

The following example shows how to use the **dhcpd enable** command to enable the DHCP server on the inside interface:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
debug dhcpd	Displays debug information for the DHCP server.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd lease

To specify the DHCP lease length, use the **dhcpd lease** command in global configuration mode. To restore the default value for the lease, use the **no** form of this command.

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
lease_length	Length of the IP address lease, in seconds, granted to the DHCP client from the DHCP server; valid values are from 300 to 1048575 seconds.

Defaults

The default *lease_length* is 3600 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd lease** command lets you specify the length of the lease, in seconds, that is granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address that the DHCP server granted.

The **no dhcpd lease** command lets you remove the lease length that you specified from the configuration and replaces this value with the default value of 3600 seconds.

Examples

The following example shows how to use the **dhcpd lease** command to specify the length of the lease of DHCP information for DHCP clients:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd option

To configure DHCP options, use the **dhcpd option** command in global configuration mode. To clear the option, use the **no** form of this command.

dhcpd option *code* {**ascii** *string*} | {**ip** *IP_address* [*IP_address*]} | {**hex** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

Syntax Description

ascii	Specifies that the option parameter is an ASCII character string.
code	A number representing the DHCP option being set. Valid values are 0 to 255 with several exceptions. See the "Usage GuidelinesUsage Guidelines" section, below, for the list of DHCP option codes that are not supported.
hex	Specifies that the option parameter is a hexadecimal string.
hex_string	Specifies a hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
ip	Specifies that the option parameter is an IP address. You can specify a maximum of two IP addresses with the **ip** keyword.
IP_address	Specifies a dotted-decimal IP address.
string	Specifies an ASCII character string without spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can use the **dhcpd option** command to provide TFTP server information to Cisco IP Phones and routers.

When a DHCP option request arrives at the security appliance DHCP server, the security appliance places the value or values that are specified by the **dhcpd option** command in the response to the client.

The **dhcpd option 66** and **dhcpd option 150** commands specify TFTP servers that Cisco IP Phones and routers can use to download configuration files. Use the commands as follows:

- **dhcpd option 66 ascii** *string*, where *string* is either the IP address or hostname of the TFTP server. Only one TFTP server can be specified for option 66.
- **dhcpd option 150 ip** *IP_address* [*IP_address*], where *IP_address* is the IP address of the TFTP server. You can specify a maximum of two IP addresses for option 150.

Note The **dhcpd option 66** command only takes an **ascii** parameter, and the **dhcpd option 150** only takes an **ip** parameter.

Use the following guidelines when specifying an IP address for the **dhcpd option 66 | 150** commands:

- If the TFTP server is located on the DHCP server interface, use the local IP address of the TFTP server.
- If the TFTP server is located on a less secure interface than the DHCP server interface, then general outbound rules apply. Create a group of NAT, global, and **access-list** entries for the DHCP clients, and use the actual IP address of the TFTP server.
- If the TFTP server is located on a more secure interface, then general inbound rules apply. Create a group of static and **access-list** statements for the TFTP server and use the global IP address of the TFTP server.

For information about other DHCP options, refer to RFC2132.

Note The security appliance does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter **dhcpd option 46 ascii hello**, and the security appliance accepts the configuration although option 46 is defined in RFC 2132 as expecting a single-digit, hexadecimal value.

You cannot configure the following DHCP options with the **dhcpd option** command:

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME

Option Code	Description
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Examples

The following example shows how to specify a TFTP server for DHCP option 66:

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd ping_timeout

To change the default timeout for DHCP ping, use the **dhcpd ping_timeout** command in global configuration mode. To return to the default value, use the **no** form of this command. To avoid address conflicts, the DHCP server sends two ICMP ping packets to an address before assigning that address to a DHCP client. This command specifies the ping timeout in milliseconds.

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
number	The timeout value of the ping, in milliseconds. The minimum value is 10, the maximum is 10000. The default is 50.

Defaults

The default number of milliseconds for *number* is 50.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance waits for both ICMP ping packets to time out before assigning an IP address to a DHCP client. For example, if the default value is used, the security appliance waits for 1500 milliseconds (750 milliseconds for each ICMP ping packet) before assigning an IP address.

A long ping timeout value can adversely affect the performance of the DHCP server.

Examples

The following example shows how to use the **dhcpd ping_timeout** command to change the ping timeout value for the DHCP server:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd update dns

To enable a DHCP server to perform Dynamic DNS updates, use the **dhcpd update dns** command in global configuration mode. To disable DDNS by a DHCP server, use the **no** form of this command.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

Syntax Description

both	Specifies that the DHCP server updates both A and PTR DNS RRs.
interface	Specifies the security appliance interface to which the DDNS updates apply.
override	Specifies that the DHCP server overrides DHCP client requests.
srv_ifc_name	Specifies an interface to apply this option to.

Defaults

By default, the DHCP server performs PTR RR updates only.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

DDNS updates the name to address and address to name mappings maintained by DNS. Updates are performed in conjunction with a DHCP server. The **dhcpd update dns** command enables updates by the server.

Name and address mappings are contained in two types of RRs:

- The A resource record contains domain name to IP address mappings.
- The PTR resource record contains IP address to domain name mappings.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

Using the **dhcpd update dns** command, the DHCP server can be configured to perform both A and PRT RR updates or PTR RR updates only. It can also be configured to override update requests from the DHCP client.

Examples

The following example configures the DDNS server to perform both A and PTR updates while also overriding requests from the DHCP client:

```
hostname(config)# dhcpd update dns both override
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a DDNS update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

dhcpd wins

To define the WINS servers for DHCP clients, use the **dhcpd wins** command in global configuration mode. To remove the WINS servers from the DHCP server, use the **no** form of this command.

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

Syntax Description

interface *if_name*	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
server1	Specifies the IP address of the primary Microsoft NetBIOS name server (WINS server).
server2	(Optional) Specifies the IP address of the alternate Microsoft NetBIOS name server (WINS server).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcpd wins** command lets you specify the addresses of the WINS servers for the DHCP client. The **no dhcpd wins** command removes the WINS server IP addresses from the configuration.

Examples

The following example shows how to use the dhcpd wins command to specify WINS server information that is sent to DHCP clients:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd dns	Defines the DNS servers for DHCP clients.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcprelay enable

To enable the DHCP relay agent, use the **dhcprelay enable** command in global configuration mode. To disable DHCP relay agent, use the **no** form of this command. The DHCP relay agent allows DHCP requests to be forwarded from a specified security appliance interface to a specified DHCP server.

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

Syntax Description

interface_name	Name of the interface on which the DHCP relay agent accepts client requests.

Defaults

The DHCP relay agent is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For the security appliance to start the DHCP relay agent with the **dhcprelay enable** *interface_name* command, you must have a **dhcprelay server** command already in the configuration. Otherwise, the security appliance displays an error message similar to the following:

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

You cannot enable DHCP relay under the following conditions:

- You cannot enable DHCP relay and the DHCP relay server on the same interface.
- You cannot enable DCHP relay and a DHCP server (**dhcpd enable**) on the same interface.
- You cannot enable DHCP relay in a context at the same time as the DHCP server.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context (a shared VLAN).

The **no dhcprelay enable** *interface_name* command removes the DHCP relay agent configuration for the interface that is specified by *interface_name* only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the security appliance, client requests on the inside interface of the security appliance, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

The following example shows how to disable the DHCP relay agent:

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcp relay	Displays debug information for the DHCP relay agent.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay server

To specify the DHCP server that DHCP requests are forwarded to, use the **dhcpreplay server** command in global configuration mode. To remove the DHCP server from the DHCP relay configuration, use the **no** form of this command. The DHCP relay agent allows DHCP requests to be forwarded from a specified security appliance interface to a specified DHCP server.

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address* [*interface_name*]

Syntax Description

interface_name	Name of the security appliance interface on which the DHCP server resides.
IP_address	The IP address of the DHCP server to which the DHCP relay agent forwards client DHCP requests.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can add up to four DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the security appliance configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration.

When you use the **no dhcprelay server** *IP_address* [*interface_name*] command, the interface stops forwarding DHCP packets to that server.

The **no dhcprelay server** *IP_address* [*interface_name*] command removes the DHCP relay agent configuration for the DHCP server that is specified by *IP_address* [*interface_name*] only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the security appliance, client requests on the inside interface of the security appliance, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay setroute

To set the default gateway address in the DHCP reply, use the **dhcprelay setroute** command in global configuration mode. To remove the default router, use the **no** form of this command. This command causes the default IP address of the DHCP reply to be substituted with the address of the specified security appliance interface.

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

Syntax Description

interface	Configures the DHCP relay agent to change the first default IP address (in the packet sent from the DHCP server) to the address of *interface*.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcprelay setroute** *interface* command lets you enable the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *interface*.

If there is no default router option in the packet, the security appliance adds one containing the address of *interface*. This action allows the client to set its default route to point to the security appliance.

When you do not configure the **dhcprelay setroute** *interface* command (and there is a default router option in the packet), it passes through the security appliance with the router address unaltered.

Examples

The following example shows how to use the **dhcprelay setroute** command to set the default gateway in the DHCP reply from the external DHCP server to the inside interface of the security appliance:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay timeout

To set the DHCP relay agent timeout value, use the **dhcprelay timeout** command in global configuration mode. To restore the timeout value to its default value, use the **no** form of this command.

dhcprelay timeout *seconds*

no dhcprelay timeout

Syntax Description

seconds	Specifies the number of seconds that are allowed for DHCP relay address negotiation.

Defaults

The default value for the dhcprelay timeout is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **dhcprelay timeout** command lets you set the amount of time, in seconds, allowed for responses from the DHCP server to pass to the DHCP client through the relay binding structure.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the security appliance, client requests on the inside interface of the security appliance, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dialog

To customize dialog messages displayed to WebVPN users, use the **dialog** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

dialog {**title** | **message** | **border**} **style** *value*

no dialog {**title** | **message** | **border**} **style** *value*

Syntax Description

border	Specifies you are changing the border.
message	Specifies you are changing the message.
style	Specifies you are changing the style.
title	Specifies you are changing the title.
value	The actual text to display (maximum 256 characters), or CSS parameters (maximum 256 characters).

Defaults

The default title style is background-color:#669999;color:white.

The default message style is background-color:#99CCCC;color:black.

The default border style is border:1px solid black;border-collapse:collapse.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the dialog message, changing the foreground color to blue:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# dialog message style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

dir

To display the directory contents, use the **dir** command in privileged EXEC mode.

dir [/all] [**all-filesystems**] [**/recursive**] [**flash:** | **system:**] [*path]*

Syntax Description

/all	(Optional) Displays all files.
all-filesystems	(Optional) Displays the files of all filesystems
disk0:	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
/recursive	(Optional) Displays the directory contents recursively.
system:	(Optional) Displays the directory contents of the file system.
flash:	(Optional) Displays the directory contents of the default Flash partition.
path	(Optional) Specifies a specific path.

Defaults

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **dir** command without keywords or arguments displays the directory contents of the current directory.

Examples

The following example shows how to display the directory contents:

```
hostname# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

The following example shows how to display recursively the contents of the entire file system:

```
hostname# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
pwd	Displays the current working directory.
mkdir	Creates a directory.
rmdir	Removes a directory.

disable

To exit privileged EXEC mode and return to unprivileged EXEC mode, use the **disable** command in privileged EXEC mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **enable** command to enter privileged mode. The **disable** command allows you to exit privileged mode and returns you to an unprivileged mode.

Examples

The following example shows how to enter privileged mode:

```
hostname> enable
hostname#
```

The following example shows how to exit privileged mode:

```
hostname# disable
hostname>
```

Related Commands

Command	Description
enable	Enables privileged EXEC mode.

disable (cache)

To disable caching for WebVPN, use the **disable** command in cache configuration mode. To reenable caching, use the **no** version of this command.

disable

no disable

Defaults

Caching is enabled with default settings for each cache attribute.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cache configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to disable caching, and how to then reenable it.

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# disable
hostname(config-webvpn-cache)# no disable
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.

Command	Description
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

disable service-settings

To disable the service settings on IP phones when using the Phone Proxy feature, use the **disable service-settings** command in phone-proxy configuration mode. To preserve the settings on the IP phones, use the **no** form of this command.

disable service-settings

no disable service-settings

Syntax Description

There are no arguments or keywords for this command.

Defaults

The service settings are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

By default, the following settings are disabled on the IP phones:

- PC Port
- Gratuitous ARP
- Voice VLAN access
- Web Access
- Span to PC Port

To preserve the settings configured on the CUCM for each IP phone configured, configure the **no disable service-settings** command.

Examples

The following example shows the use of the **disable service-settings** command to preserve the settings of the IP phones that use the Phone Proxy feature on the ASA:

```
hostname(config-phone-proxy)# no disable service-settings
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
show phone-proxy	Displays Phone Proxy specific information.

display

To display attribute value pairs that the security appliance writes to the DAP attribute database, enter the **display** command in dap test attributes mode.

display

Command Default

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
dap test attributes	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Normally the security appliance retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The security appliance writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record. The **display** command lets you display these attributes to the console.

Related CommandsI

Command	Description
attributes	Enters attributes mode, in which you can set attribute value pairs.
dynamic-access-policy-record	Creates a DAP record.
test dynamic-access-policy attributes	Enters attributes submode.
test dynamic-access-policy execute	Executes the logic that generates the DAP and displays the resulting access policies to the console.

distance eigrp

To configure the administrative distances of internal and external EIGRP routes, use the **distance eigrp** command in router configuration mode. To restore the default values, use the **no** form of this command.

distance eigrp *internal-distance external-distance*

no distance eigrp

Syntax Description

external-distance	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values are from 1 to 255.
internal-distance	Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values are from 1 to 255.

Defaults

The default values are as follows:

- *external-distance* is 170
- *internal-distance* is 90

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Because every routing protocol has metrics based on algorithms that are different from the other routing protocols, it is not always possible to determine the “best path” for two routes to the same destination that were generated by different routing protocols. Administrative distance is a route parameter that the security appliance uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.

If you have more than one routing protocol running on the security appliance, you can use the **distance eigrp** command to adjust the default administrative distances of routes discovered by the EIGRP routing protocol in relation to the other routing protocols. Table 11-1 lists the default administrative distances for the routing protocols supported by the security appliance.

Table 11-1 Default Administrative Distances

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
Internal EIGRP	90
OSPF	110
RIP	120
EIGRP external route	170
Unknown	255

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for both internal and external EIGRP routes.

Examples

The following example uses the **distance eigrp** command set the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 115. Setting the EIGRP external route administrative distance to 115 would give routes discovered by EIGRP to a specific destination preference over the same routes discovered by RIP but not by OSPF.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.7.0
hostname(config-router)# network 172.16.0.0
hostname(config-router)# distance eigrp 90 115
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

distance ospf

To define OSPF route administrative distances based on route type, use the **distance ospf** command in router configuration mode. To restore the default values, use the **no** form of this command.

distance ospf [**intra-area** *d1*] [**inter-area** *d2*] [**external** *d3*]

no distance ospf

Syntax Description

d1, *d2*, and *d3*	Distance for each route types. Valid values range from 1 to 255.
external	(Optional) Sets the distance for routes from other routing domains that are learned by redistribution.
inter-area	(Optional) Sets the distance for all routes from one area to another area.
intra-area	(Optional) Sets the distance for all routes within an area.

Defaults

The default values for *d1*, *d2*, and *d3* are 110.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You must specify at least one keyword and argument. You can enter the commands for each type of administrative distance separately, however they appear as a single command in the configuration. If you reenter an administrative distance, the administrative distance for only that route type changes; the administrative distances for any other route types remain unaffected.

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for all of the route types. If you want to restore the default administrative distance for a single route type when you have multiple route types configured, you can do one of the following:

- Manually set that route type to the default value.
- Use the **no** form of the command to remove the entire configuration and then re-enter the configurations for the route types you want to keep.

Examples

The following example sets the administrative distance of external routes to 150:

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

The following example shows how entering separate commands for each route type appears as a single command in the router configuration:

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

The following example shows how to set each administrative distance to 105, and then change only the external administrative distance to 150. The **show running-config router ospf** command shows how only the external route type value changed, while the other route types retained the value previously set.

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

distribute-list in

To filter the networks received in routing updates, use the **distribute-list in** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

Syntax Description

acl	Name of a standard access list.
if_name	(Optional) The interface name as specified by the **nameif** command. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Defaults

Networks are not filtered in incoming updates.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters RIP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
hostname(config)# access-list ripfilter permit 10.0.0.0
hostname(config)# access-list ripfilter deny any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter in interface outside
```

The following example filters EIGRP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
hostname(config)# access-list eigrp_filter permit 10.0.0.0
hostname(config)# access-list eigrp_filter deny any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
```

```
hostname(config-router)# distribute-list eigrp_filter in interface outside
```

Related Commands

Command	Description
distribute-list out	Filters networks from being advertised in routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list out

To filter specific networks from being sent in routing updates, use the **distribute-list out** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name* | **eigrp** *as_number* | **rip** | **ospf** *pid* | **static** | **connected**]

Syntax Description

acl	Name of a standard access list.
connected	(Optional) Filters only connected routes.
eigrp *as_number*	(Optional) Filters only EIGRP routes from the specified autonomous system number. The *as_number* is the autonomous system number of the EIGRP routing process on the security appliance.
interface *if_name*	(Optional) The interface name as specified by the **nameif** command. Specifying an interface causes the access list to be applied only to routing updates sent on the specified interface.
ospf *pid*	(Optional) Filters only OSPF routes discovered by the specified OSPF process.
rip	(Optional) Filters only RIP routes.
static	(Optional) Filters only static routes

Defaults

Networks are not filtered in sent updates.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	The **eigrp** keyword was added.

Usage Guidelines

If no interface is specified, the access list will be applied to all outgoing updates.

Examples

The following example prevents the 10.0.0.0 network from being advertised in RIP updates sent out of any interface:

```
hostname(config)# access-list ripfilter deny 10.0.0.0
hostname(config)# access-list ripfilter permit any
```

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter out
```

The following example prevents the EIGRP routing process from advertising the 10.0.0.0 network on the outside interface:

```
hostname(config)# access-list eigrp_filter deny 10.0.0.0
hostname(config)# access-list eigrp_filter permit any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list eigrp_filter out interface outside
```

Related Commands

Command	Description
distribute-list in	Filters networks received in routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
router rip	Enters router configuration mode for the RIP routing process.
show running-config router	Displays the commands in the global router configuration.

dns domain-lookup

To enable the security appliance to send DNS requests to a DNS server to perform a name lookup for supported commands, use the **dns domain-lookup** command in global configuration mode. To disable DNS lookup, use the **no** form of this command.

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

Syntax Description

interface_name	Specifies the interface on which you want to enable DNS lookup. If you enter this command multiple times to enable DNS lookup on multiple interfaces, the security appliance tries each interface in order until it receives a response.

Defaults

DNS lookup is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **dns name-server** command to configure the DNS server addresses to which you want to send DNS requests. See the **dns name-server** command for a list of commands that support DNS lookup.

The security appliance maintains a cache of name resolutions that consists of dynamically learned entries. Instead of making queries to external DNS servers each time an hostname-to-IP-address translation is needed, the security appliance caches information returned from external DNS requests. The security appliance only makes requests for names that are not in the cache. The cache entries time out automatically according to the DNS record expiration, or after 72 hours, whichever comes first.

Examples

The following example enables DNS lookup on the inside interface:

```
hostname(config)# dns domain-lookup inside
```

Related Commands

Command	Description
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns-group (tunnel-group webvpn configuration mode)

To specify the DNS server to use for a WebVPN tunnel-group, use the **dns-group** command in tunnel-group webvpn configuration mode. To restore the default DNS group, use the **no** form of this command.

dns-group *name*

no dns-group

Syntax Description

name	Specifies the name of the DNS server group configuration to use for the tunnel group.

Defaults

The default value is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The name can specify any DNS group. The dns-group command resolves the hostname to the appropriate DNS server for the tunnel group.

You configure the DNS group using the **dns server-group** command.

Examples

The following example shows a customization command that specifies the use of the DNS group named "dnsgroup1":

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group dnsgroup1
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters DNS-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

dns-guard

To enable the DNS guard function, which enforces one DNS response per query, use the **dns-guard** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

dns-guard

no dns-guard

Syntax Description

This command has no arguments or keywords.

Defaults

DNS guard is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no dns-guard** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, the behavior is determined by the **global dns-guard** command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The indentification field in the DNS header is used to match the DNS response with the DNS header. One response per query is allowed through the security appliance.

Examples

The following example shows how to enable DNS guard in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

dns retries

To specify the number of times to retry the list of DNS servers when the security appliance does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

dns retries *number*

no dns retries [*number*]

Syntax Description

number	Specifies the number of retries between 0 and 10. The default is 2.

Defaults

The default number of retries is 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated for WebVPN connections.

Usage Guidelines

Add DNS servers using the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The security appliance only tries each server one time.

```
hostname(config)# dns retries 0
hostname(config)#
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

Command	Description
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns-server

To set the IP address of the primary and secondary DNS servers, use the **dns-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

dns-server {**value** *ip_address* [*ip_address*] | none}

no dns-server

Syntax Description

none	Sets dns-servers to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary DNS servers.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This option allows inheritance of a DNS server from another group policy. To prevent inheriting a server, use the **dns-server none** command.

Every time you issue the **dns-server** command you overwrite the existing setting. For example, if you configure DNS server x.x.x.x and then configure DNS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole DNS server. The same holds true for multiple servers. To add a DNS server rather than overwrite previously configured servers, include the IP addresses of all DNS servers when you enter this command.

Examples

The following example shows how to configure DNS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup.

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

dns server-group

To enter the dns server-group mode, in which you can specify the domain-name, name-server, number of retries, and timeout values for a DNS server to use for a tunnel-group, use the **dns server-group** command in global configuration mode. To remove a particular DNS server group, use the **no** form of this command.

dns server -group *name*

no dns server-group

Syntax Description

name	Specifies the name of the DNS server group configuration to use for the tunnel group.

Defaults

The default value is DefaultDNS.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The name can specify any DNS group. You configure the DNS group using the **dns server-group** command.

Examples

The following example configures a DNS server group named “eval”:

```
hostname(config)# dns server-group eval
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 192.168.10.10
hostname(config-dns-server-group)# retries 5
hostname(config-dns-server-group)# timeout 7
hostname(config-dns-server-group)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
show running-config dns server-group	Shows the current running DNS server-group configuration.

dns timeout

To specify the amount of time to wait before trying the next DNS server, use the **dns timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

dns timeout *seconds*

no dns timeout [*seconds*]

Syntax Description

seconds	Specifies the timeout in seconds between 1 and 30. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles. See the **dns retries** command to configure the number of retries.

Defaults

The default timeout is 2 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the timeout to 1 second:

```
hostname(config)# dns timeout 1
```

Related Commands

Command	Description
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns domain-lookup	Enables the security appliance to perform a name lookup.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

domain-name

To set the default domain name, use the **domain-name** command in global configuration mode. To remove the domain name, use the **no** form of this command. The security appliance appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com," and specify a syslog server by the unqualified name of "jupiter," then the security appliance qualifies the name to "jupiter.example.com."

domain-name *name*

no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Defaults

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Examples

The following example sets the domain as example.com:

```
hostname(config)# domain-name example.com
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.

Command	Description
hostname	Sets the security appliance hostname.
show running-config domain-name	Shows the domain name configuration.

domain-name (dns server-group)

To set the default domain name, use the **domain-name** command in dns server-group configuration mode. To remove the domain name, use the **no** form of this command. The security appliance appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com," and specify a syslog server by the unqualified name of "jupiter," then the security appliance qualifies the name to "jupiter.example.com."

domain-name *name*

no domain-name [*name*]

Syntax Description

name	Sets the domain name, up to 63 characters.

Defaults

The default domain name is default.domain.invalid.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
dns server-group configuration	•	•	•	•	•

Command History

Release	Modification
7.1(1)	This command replaces the **dns domain-lookup** command, which is deprecated.

Usage Guidelines

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Examples

The following example sets the domain as "example.com" for "dnsgroup1":

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# domain-name example.com
hostname(config-dns-server-group)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters DNS-server-group mode, in which you can configure a DNS server group.

Command	Description
domain-name	Sets the default domain name globally.
show running-config dns-server group	Shows one or all the current DNS server-group configurations.

downgrade

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.

Caution Do not load a previous version of the software if your PIX security appliance is currently running PIX Version 7.0 or later. Loading a software image from monitor mode, on a PIX security appliance that has a PIX Version 7.0 file system, results in unpredictable behavior and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

downgrade *image_url* **[activation-key [flash |** *4-part_key* **|** *file***]] [config** *start_config_url***]**

Syntax Description

4-part_key	(Optional) Specifies the four-part activation key to write to the image. If you are using a five-part key, a warning with the list of features that might be lost by going back to the four-part key is generated. If the system Flash has been reformatted or erased, no default key is available for the downgrade. In that case, the CLI prompts you to enter an activation key at the command line. This is the default behavior if the **activation-key** keyword is not specified at the command line.
activation-key	(Optional) Specifies the activation key to use with the downgraded software image.
config	(Optional) Specifies the startup configuration file.
file	(Optional) Specifies the path/URL and name of the activation key file to use after the downgrade procedure completes. If the source image file is the one saved in Flash during the upgrade process, the activation key in this file is used with the downgrade.
flash	(Optional) Specifies to look in flash memory for the four-part activation key that was used on the device prior to using a five-part activation key. This is the default behavior if the **activation-key** keyword is not specified at the command line.
image_url	Specifies the path/URL and name of the software image to downgrade to. The software image must be a version prior to 7.0.
start_config_url	(Optional) Specifies the path/URL and name of the configuration file to use after the downgrade procedure completes.

Defaults

If the **activation-key** keyword is not specified, the security appliance tries to use the last four-part activation key used. If the security appliance cannot find a four-part activation key in Flash, the command is rejected and an error message displays. In this case, a valid four-part activation-key must be specified at the command line next time. The default activation key or the user specified activation key is compared with the activation key currently in effect. If there is a potential loss of features by using the chosen activation key, a warning displays with the list of features that could be lost after downgrade.

The security appliance uses downgrade.cfg by default if the startup configuration file is not specified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•		

Command History

Version	Modification
7.0	This command was introduced.

Usage Guidelines

This command is available only on Cisco PIX Firewall series security appliances running software Version 7.0 and later. This command is not supported on Cisco ASA 5500 series security appliances.

Caution A power failure during the downgrade process might corrupt the flash memory. As a precaution, backup all data on the flash memory to an external device prior to starting the downgrade process.

Recovering corrupt flash memory requires direct console access. See the **format** command for more information.

Examples

The following example downgrades the software to Version 6.3.3:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded
```

```
Rebooting....

Enter zero actkey:
```

The following example shows what happens if you enter an invalid activation key:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

The following example shows what happens if you specify an image and do not verify the activation key:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

The following example shows what happens if the four-part activation key does not have all the features that the current five-part activation key has:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

Related Commands

Command	Description
copy running-config startup-config	Saves the current running configuration to flash memory.

download-max-size

To specify the maximum size allowed for an object to download, use the **download-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

download-max-size <*size*>

no download-max-size

Syntax Description

size	Specifies the maximum size allowed for a downloaded object. The range is 0 through 2147483647.

Defaults

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Setting the size to 0 effectively disallows object downloading.

Examples

The following example sets the maximum size for a downloaded object to 1500 bytes:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# download-max-size 1500
```

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
upload-max-size	Specifies the maximum size of an object to upload.

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

drop

To drop all packets that match the **match** command or **class** command, use the drop command in match or class configuration mode. To disable this action, use the **no** form of this command.

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

Syntax Description

send-protocol-error	Sends a protocol error message.
log	Logs the match. The system log message number depends on the application.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When using the Modular Policy Framework, drop packets that match a **match** command or class map by using the **drop** command in match or class configuration mode. This drop action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop** command to drop all packets that match the **match** command or **class** command.

If you drop a packet, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

drop-connection

When using the Modular Policy Framework, drop packets and close the connection for traffic that matches a **match** command or class map by using the **drop-connection** command in match or class configuration mode. The connection will be removed from the connection database on the security appliance. Any subsequent packets entering the security appliance for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the **no** form of this command.

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

Syntax Description

send-protocol-error	Sends a protocol error message.
log	Logs the match. The system log message number depends on the application.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop-connection** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you drop a packet or close a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet and close the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop-connection** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example drops packets, closes the connection, and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

dtls port

To specify a port for DTLS connections, use the **dtls port** command from webvpn configuration mode. To remove the command from the configuration, use the **no** form of this command:

dtls port *number*

no dtls port *number*

Syntax Description

number	The UDP port number, from 1 to 65535.

Defaults

The default port number is 443.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command specifies the UDP port to be used for SSL VPN connections using DTLS.

DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Examples

The following example enters webvpn configuration mode and specifies port 444 for DTLS:

```
hostname(config)# webvpn
hostname(config-webvpn)# dtls port 444
```

Related Commands

Command	Description
dtls enable	Enables DTLS on an interface.
svc dtls	Enables DTLS for groups or users establishing SSL VPN connections.
vpn-tunnel-protocol	Specifies VPN protocols that the security appliance allows for remote access, including SSL.

duplex

To set the duplex of a copper (RJ-45) Ethernet interface, use the **duplex** command in interface configuration mode. To restore the duplex setting to the default, use the **no** form of this command.

duplex {**auto** | **full** | **half**}

no duplex

Syntax Description

auto	Auto-detects the duplex mode.
full	Sets the duplex mode to full duplex.
half	Sets the duplex mode to half duplex.

Defaults

The default is auto detect.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the duplex mode on the physical interface only.

The **duplex** command is not available for fiber media.

If your network does not support auto detection, set the duplex mode to a specific value.

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the duplex to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the duplex mode to full duplex:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

dynamic-access-policy-config

To configure a DAP record and the access policy attributes associated with it, use the **dynamic-access-policy-config** command in global configuration mode. To remove an existing DAP configuration, use the **no** form of this command.

To activate a DAP selection configuration file, use the **dynamic-access-policy-config** command with the activate argument.

dynamic-access-policy-config *name* | *activate*

no dynamic-access-policy-config

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.
activate	Activates the DAP selection configration file

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Name - Global configuration Activeate - Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the dynamic-access-policy-config command in global configuration mode to create one or more DAP records. When you use this command you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- action
- description
- network-acl
- priority
- user-message
- webvpn

Examples

The following example shows how to configure the DAP record named user1.

```
hostname(config)# dynamic-access-policy-config user1
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Populates the DAP record with access policy attributes.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

dynamic-access-policy-record

To create a DAP record and populate it with access policy attributes, use the **dynamic-access-policy-record** command in global configuration mode. To remove an existing DAP record, use the **no** form of this command.

dynamic-access-policy-record *name*

no dynamic-access-policy-record *name*

Syntax Description

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the dynamic-access-policy-record command in global configuration mode to create one or more DAP records. When you use this command you enter dynamic-access-policy-record mode, in which you can set attributes for the named DAP record. The commands you can use in dynamic-access-policy-record mode include the following:

- action
- description
- network-acl
- priority
- user-message
- webvpn

Examples

The following example shows how to create a DAP record named Finance.

```
hostname(config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
clear config dynamic-access-policy-record [*name*]	Removes all DAP records or the named DAP record.
dynamic-access-policy-config url	Configures the DAP Selection Configuration file.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

CHAPTER 12

eigrp log-neighbor-changes through functions (removed) Commands

eigrp log-neighbor-changes

To enable the logging of EIGRP neighbor adjacency changes, use the **eigrp log-neighbor-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eigrp log-neighbor-changes** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor changes:

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-changes
```

Related Commands

Command	Description
eigrp log-neighbor-warnings	Enables logging of neighbor warning messages.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp log-neighbor-warnings

To enable the logging of EIGRP neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. Valid values are from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Defaults

This command is enabled by default. All neighbor warning messages are logged.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eigrp log-neighbor-warnings** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor warning messages:

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-warnings
```

The following example logs EIGRP neighbor warning messages and repeats the warning messages in 5-minute (300 seconds) intervals:

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
eigrp log-neighbor-messages	Enables the logging of changes in EIGRP neighbor adjacencies.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp router-id

To specify router ID used by the EIGRP routing process, use the **eigrp router-id** command in router configuration mode. To restore the default value, use the **no** form of this command.

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

Syntax Description

ip-addr	Router ID in IP address (dotted-decimal) format. You cannot use 0.0.0.0 or 255.255.255.255 as the router ID.

Defaults

If not specified, the highest-level IP address on the security appliance is used as the router ID.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If the **eigrp router-id** command is not configured, EIGRP automatically selects the highest IP address on the security appliance to use as the router ID when an EIGRP process is started.The router ID is not changed unless the EIGRP process is removed using the **no router eigrp** command or unless the router ID is manually configured with the **eigrp router-id** command.

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. To prevent this, use the **eigrp router-id** command to specify a global address for the router ID.

A unique value should be configured for each EIGRP router.

Examples

The following example configures 172.16.1.3 as a fixed router ID for the EIGRP routing process:

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp stub

To configure the EIGRP routing process as a stub routing process, use the **eigrp stub** command in router configuration mode. To remove EIGRP stub routing, use the **no** form of this command.

eigrp stub [**receive-only]** | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [receive-only] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

Syntax Description

connected	(Optional) Advertises connected routes.
receive-only	(Optional) Sets the security appliance as a received-only neighbor.
redistributed	(Optional) Advertises routes redistributed from other routing protocols.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.

Defaults

Stub routing is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **eigrp stub** command to configure the security appliance as a stub where the security appliance directs all IP traffic to a distribution router.

Using the **receive-only** keyword restricts the security appliance from sharing any of its routes with any other router in the autonomous system; the security appliance only receives updates from the EIGRP neighbor. You cannot use any other keyword with the **receive-only** keyword.

You can specify one or more of the **connected**, **static**, **summary**, and **redistributed** keywords. If any of these keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword are sent.

The **connected** keyword permits the EIGRP stub routing process to send connected routes. If the connected routes are not covered by a **network** statement, it may be necessary to redistribute connected routes with the **redistribute** command under the EIGRP process.

The **static** keyword permits the EIGRP stub routing process to send static routes. Without the configuration of this option, EIGRP will not send any static routes. If the static routes are not covered by a **network** statement, it may be necessary to redistribute them with the **redistribute** command under the EIGRP process.

The **summary** keyword permits the EIGRP stub routing process to send summary routes. You can create summary routes manually with the **summary-address eigrp** command or automatically with the **auto-summary** command enabled (**auto-summary** is enabled by default).

The **redistributed** keyword permits the EIGRP stub routing process to send routes redistributed into the EIGRP routing process from other routing protocols. If you do you configure this option, EIGRP does not advertise redistributed routes.

Examples

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises connected and summary routes:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected summary
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises connected and static routes. Sending summary routes is not permitted.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected static
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that only receives EIGRP updates. Connected, summary, and static route information is not sent.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 eigrp
hostname(config-router)# eigrp stub receive-only
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises routes redistributed into EIGRP from other routing protocols:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub redistributed
```

The following example uses the **eigrp stub** command without any of the optional arguments. When used without arugments, the **eigrp stub** commands advertises connected and static routes by default.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub
```

Related Commands

Command	Description
router eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

eject

To support the removal of an ASA 5500 series external compact Flash device, use the **eject** command in user EXEC mode.

eject [*/noconfirm*] *disk1:*

Syntax Description

disk1:	Specifies the device to eject.
/noconfirm	Specifies that you do not need to confirm device removal before physically removing the external Flash device from the security appliance.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eject** command allows you to safely remove a compact Flash device from an ASA 5500 series security appliance.

The following example shows how to use the **eject** command to shut down *disk1* gracefully before the device is physically removed from the security appliance:

```
hostname# eject /noconfig disk1:
It is now safe to remove disk1:
hostname# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

email

To include the indicated email address in the Subject Alternative Name extension of the certificate during enrollment, use the **email** command in crypto ca-trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

email *address*

no email

Syntax Description

address	Specifies the email address. The maximum length of *address* is 64 characters.

Defaults

The default setting is not set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca-trustpoint configuration	•	•	•		

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and includes the email address user1@user.net in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca-trustpoint central
hostname(ca-trustpoint)# email user1@user.net
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca-trustpoint	Enters trustpoint configuration mode.

enable

To enter privileged EXEC mode, use the **enable** command in user EXEC mode.

enable [*level*]

Syntax Description

level	(Optional) The privilege level between 0 and 15. Not used with enable authentication (the **aaa authentication enable console** command).

Defaults

Enters privilege level 15 unless you are using enable authentication (using the **aaa authentication enable console** command), in which case the default level depends on the level configured for your username.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The default enable password is blank. See the **enable password** command to set the password.

Without enable authentication, when you enter the **enable** command, your username changes to enable_*level*, where the default level is 15. With enable authentication (using the **aaa authentication enable console** command), the username and associated level are preserved. Preserving the username is important for command authorization (the **aaa authorization command** command, using either local or TACACS+).

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode. To use levels in between, enable local command authorization (the **aaa authorization command LOCAL** command) and set the commands to different privilege levels using the **privilege** command. TACACS+ command authorization does not use the privilege levels configured on the security appliance.

See the **show curpriv** command to view your current privilege level.

Enter the **disable** command to exit privileged EXEC mode.

Examples

The following example enters privileged EXEC mode:

```
hostname> enable
Password: Pa$$w0rd
hostname#
```

The following example enters privileged EXEC mode for level 10:

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

Related Commands

Command	Description
enable password	Sets the enable password.
disable	Exits privileged EXEC mode.
aaa authorization command	Configures command authorization.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.

enable (webvpn)

To enable WebVPN or e-mail proxy access on a previously configured interface, use the enable command. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S. POP3S, SMTPS), use this command in the applicable e-mail proxy mode. To disable WebVPN on an interface, use the **no** version of the command.

enable *ifname*

no enable

Syntax Description

ifname	Identifies the previously configured inteface. Use the **nameif** command to configure interfaces.

Defaults

WebVPN is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enable WebVPN on the interface named Outside:

```
hostname(config)# webvpn
hostname(config-webvpn)# enable Outside
```

The following example shows how to configure POP3S e-mail proxy on the interface named Outside:

```
hostname(config)# pop3s
hostname(config-pop3s)# enable Outside
```

enable gprs

To enable GPRS with RADIUS accounting, use the **enable gprs** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command. The security appliance checks for the 3GPP VSA 26-10415 in the Accounting-Request Stop messages to properly handle secondary PDP contexts. To disable this command, use the **no** form of this command.

enable gprs

no enable gprs

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This option is disabled by default. A GTP license is required to enable this feature.

Examples

The following example shows how to enable GPRS with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

enable password

To set the enable password for privileged EXEC mode, use the **enable password** command in global configuration mode. To remove the password for a level other than 15, use the **no** form of this command. You cannot remove the level 15 password.

enable password *password* **[level** *level*] [**encrypted**]

no enable password level *level*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **enable password** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config enable** command.
level *level*	(Optional) Sets a password for a privilege level between 0 and 15.
password	Sets the password as a case-sensitive string of up to 16 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

Defaults

The default password is blank. The default level is 15.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The default password for enable level 15 (the default level) is blank. To reset the password to be blank, do not enter any text for the *password*.

For multiple context mode, you can create an enable password for the system configuration as well as for each context.

To use privilege levels other than the default of 15, configure local command authorization (see the **aaa authorization command** command and specify the **LOCAL** keyword), and set the commands to different privilege levels using the **privilege** command. If you do not configure local command authorization, the enable levels are ignored, and you have access to level 15 regardless of the level you set. See the **show curpriv** command to view your current privilege level.

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode.

Examples

The following example sets the enable password to Pa$$w0rd:

```
hostname(config)# enable password Pa$$w0rd
```

The following example sets the enable password to Pa$$w0rd10 for level 10:

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

The following example sets the enable password to an encrypted password that you copied from another security appliance:

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
aaa authorization command	Configures command authorization.
enable	Enters privileged EXEC mode.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config enable	Shows the enable passwords in encrypted form.

endpoint

To add an endpoint to an HSI group for H.323 protocol inspection, use the **endpoint** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

Syntax Description

if_name	The interface through which the endpoint is connected to the security appliance.
ip_address	IP address of the endpoint to add. A maximum of ten endpoints per HSI group is allowed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HSI group configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to add endpoints to an HSI group in an H.323 inspection policy map:

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
hsi-group	Creates an HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

endpoint-mapper

To configure endpoint mapper options for DCERPC inspection, use the **endpoint-mapper** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

Syntax Description

epm-service-only	Specifies to enforce endoint mapper service during binding.
lookup-operation	Specifies to enable lookup operation of the endpoint mapper service.
timeout *value*	Specifies the timeout for pinholes from the lookup operation. Range is from 0:0:1 to 1193:0:0.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure the endpoint mapper in a DCERPC policy map:

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in ca-crl configuration mode. To permit a lapsed or missing NextUpdate field, use the **no** form of this command.

enforcenextupdate

no enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is enforced (on).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca-crl configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If set, this command requires CRLs to have a NextUpdate field that has not yet lapsed. If not used, the security appliance allows a missing or lapsed NextUpdate field in a CRL.

Examples

The following example enters ca-crl configuration mode, and requires CRLs to have a NextUpdate field that has not expired for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

Related Commands

Command	Description
cache-time	Specifies a cache refresh time in minutes.
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local ca server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval *timeout*

no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from one to 720 hours.

Defaults

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has **otp expiration** amount of time to enroll with that password. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned by way of the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the **enrollment-retrieval** command time period.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

The following example resets the retrieval time back to the default of 24 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

enrollment retry count

To specify a retry count, use the **enrollment retry count** command in crypto ca-trustpoint configuration mode. After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the configured retry period, it sends another certificate request. The security appliance repeats the request until either it receives a response or reaches the end of the configured retry period. To restore the default setting of the retry count, use the **no** form of the command.

enrollment retry count *number*

no enrollment retry count

Syntax Description

number	The maximum number of attempts to send an enrollment request. The valid range is 0, 1-100 retries.

Defaults

The default setting for *number* is 0 (unlimited).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca-trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and configures an enrollment retry count of 20 retries within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

enrollment retry period

To specify a retry period, use the **enrollment retry period** command in crypto ca trustpoint configuration mode. After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the specified retry period, it sends another certificate request. To restore the default setting of the retry period, use the **no** form of the command.

enrollment retry period *minutes*

no enrollment retry period

Syntax Description

minutes	The number of minutes between attempts to send an enrollment request. The valid range is 1- 60 minutes.

Defaults

The default setting is 1 minute.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and configures an enrollment retry period of 10 minutes within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns all enrollment parameters to their system default values.
enrollment retry count	Defines the number of retries to requesting an enrollment.

enrollment terminal

To specify cut and paste enrollment with this trustpoint (also known as manual enrollment), use the **enrollment terminal** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca-trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and specifies the cut and paste method of CA enrollment for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.
enrollment url	Specifies automatic enrollment (SCEP) with this trustpoint and configures the URL.

enrollment url

To specify automatic enrollment (SCEP) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment url** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment url *url*

no enrollment url

Syntax Description

url	Specifies the name of the URL for automatic enrollment. The maximum length is 1K characters (effectively unbounded).

Defaults

The default setting is off.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca-trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and specifies SCEP enrollment at the URL https://enrollsite for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local ca server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval *timeout*

no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from one to 720 hours.

Defaults

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has **otp expiration** amount of time to enroll with that password. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned by way of the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the **enrollment-retrieval** command time period.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

The following example resets the retrieval time back to the default of 24 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

eou allow

To enable clientless authentication in a NAC Framework configuration, use the **eou allow** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

eou allow {audit | clientless | none}

no eou allow {audit | clientless | none}

Syntax Description

audit	An audit server performs clientless authentication.
clientless	A Cisco ACS performs clientless authentication.
none	Disables clientless authentication.

Defaults

The default configuration contains the **eou allow clientless** configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	Added the audit option.
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance uses this command only if both of the following are true:

- The group policy is configured to use a nac-framework NAC policy type.
- A host on the session does not respond to EAPoUDP requests.

Examples

The following example enables the use of an ACS to perform clientless authentication:

```
hostname(config)# eou allow clientless
hostname(config)#
```

The following example shows how to configure the security appliance to use an audit server to perform clientless authentication:

```
hostname(config)# eou allow audit
hostname(config)#
```

The following example shows how to disable the use of an audit server:

```
hostname(config)# no eou allow clientless
hostname(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou clientless	Changes the username and password to be sent to the ACS for clientless authentication in a NAC Framework configuration.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou clientless

To change the username and password to be sent to the Access Control Server for clientless authentication in a NAC Framework configuration, use the **eou clientless** command in global configuration mode. To use the default value, use the **no** form of this command.

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

Syntax Description

password	Enter to change the password sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
password	Enter the password configured on the Access Control Server to support clientless hosts. Enter 4 – 32 ASCII characters.
username	Enter to change the username sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
username	Enter the username configured on the Access Control Server to support clientless hosts. Enter 1 to 64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >).

Defaults

The default value for both the username and password attributes is clientless.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the security appliance.
- Network Admission Control is configured on the security appliance.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the username for clientless authentication to sherlock:

```
hostname(config)# eou clientless username sherlock
```

```
hostname(config)#
```

The following example changes the username for clientless authentication to the default value, clientless:

```
hostname(config)# no eou clientless username
hostname(config)#
```

The following example changes the password for clientless authentication to secret:

```
hostname(config)# eou clientless password secret
hostname(config)#
```

The following example changes the password for clientless authentication to the default value, clientless:

```
hostname(config)# no eou clientless password
hostname(config)#
```

Related Commands

Command	Description
eou allow	Enables clientless authentication in a NAC Framework configuration.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.

eou initialize

To clear the resources assigned to one or more NAC Framework sessions and initiate a new, unconditional posture validation for each of the sessions, use the **eou initialize** command in privileged EXEC mode.

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

Syntax Description

all	Revalidates all NAC Framework sessions on this security appliance
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Defaults

No default behavior or values.

Command Modes

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command if a change occurs in the posture of the remote peers or if the assigned access policies (that is, the downloaded ACLs) change, and you want to clear the resources assigned to the sessions. Entering this command purges the EAPoUDP associations and access policies used for posture validation. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example initializes all NAC Framework sessions:

```
hostname# eou initialize all
hostname
```

The following example initializes all NAC Framework sessions assigned to the tunnel group named tg1:

```
hostname# eou initialize group tg1
hostname
```

The following example initializes the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
hostname# eou initialize 209.165.200.225
hostname
```

Related Commands

Command	Description
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

eou max-retry

To change the number of times the security appliance resends an EAP over UDP message to the remote computer, use the **eou max-retry** command in global configuration mode. To use the default value, use the **no** form of this command.

eou max-retry *retries*

no eou max-retry

Syntax Description

retries	Limits the number of consecutive retries sent in response to retransmission timer expirations. Enter a value in the range 1 to 3.

Defaults

The default value is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the security appliance.
- Network Admission Control is configured on the security appliance.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example limits the number of EAP over UDP retransmissions to 1:

```
hostname(config)# eou max-retry 1
hostname(config)#
```

The following example changes the number of EAP over UDP retransmissions to its default value, 3:

```
hostname(config)# no eou max-retry
hostname(config)#
```

Related Commands

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou port

To change the port number for EAP over UDP communication with the Cisco Trust Agent in a NAC Framework configuration, use the **eou port** command in global configuration mode. To use the default value, use the **no** form of this command.

eou port *port_number*

no eou port

Syntax Description

port_number	Port number on the client endpoint to be designated for EAP over UDP communications. This number is the port number configured on the Cisco Trust Agent. Enter a value in the range 1024 to 65535.

Defaults

The default value is 21862.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the port number for EAP over UDP communication to 62445:

```
hostname(config)# eou port 62445
hostname(config)#
```

The following example changes the port number for EAP over UDP communication to its default value:

```
hostname(config)# no eou port
hostname(config)#
```

Related Commands

debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
show vpn-session_summary.db	Displays the number IPSec, Cisco AnyConnect, and NAC sessions, including VLAN mapping session data.
show vpn-session.db	Displays information about VPN sessions, including VLAN mapping and NAC results.

eou revalidate

To force immediate posture revalidation of one or more NAC Framework sessions, use the **eou revalidate** command in privileged EXEC mode.

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

Syntax Description

all	Revalidates all NAC Framework sessions on this security appliance
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Defaults

No default behavior or values.

Command Modes

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. The command initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you entered the command remain in effect until the new posture validation succeeds or fails. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example revalidates all NAC Framework sessions:

```
hostname# eou revalidate all
hostname
```

The following example revalidates all NAC Framework sessions assigned to the tunnel group named tg-1:

```
hostname# eou revalidate group tg-1
hostname
```

The following example revalidates the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

Related Commands

Command	Description
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.

eou timeout

To change the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration, use the **eou timeout** command in global configuration mode. To use the default value, use the **no** form of this command.

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

Syntax Description

hold-period	Maximum time to wait after sending EAPoUDP messages equal to the number of EAPoUDP retries. The **eou initialize** or **eou revalidate** command also clears this timer. If this timer expires, the security appliance initiates a new EAP over UDP association with the remote host.
retransmit	Maximum time to wait after sending an EAPoUDP message. A response from the remote host clears this timer. The **eou initialize** or **eou revalidate** command also clears this timer. If the timer expires, the security appliance retransmits the EAPoUDP message to the remote host.
seconds	Number of seconds for the security appliance to wait. Enter a value in the range 60 to 86400 for the hold-period attribute, or the range 1 to 60 for the retransmit attribute.

Defaults

The default value of the hold-period attribute is 180.

The default value of the retransmit attribute is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the wait period before initiating a new EAP over UDP association to 120 seconds:

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

The following example changes the wait period before initiating a new EAP over UDP association to its default value:

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

The following example changes the retransmission timer to 6 seconds:

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

The following example changes the retransmission timer to its default value:

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou max-retry	Changes the number of times the security appliance resends an EAP over UDP message to the remote computer.

erase

To erase and reformat the file system, use the **erase** command in privileged EXEC mode. This command overwrites all files and erases the file system, including hidden system files, and then reinstalls the file system.

erase [**disk0: | disk1: | flash:]**

Syntax Description

disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external, compact Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. **Caution** Erasing the Flash memory also removes the licensing information, which is stored in Flash memory. Save the licensing information prior to erasing the Flash memory. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **erase** command erases all data on the Flash memory using the OxFF pattern and then rewrites an empty file system allocation table to the device.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **erase** command.

Note On Cisco PIX security appliances, the **erase** and **format** commands do the same thing, destroy user data with the 0xFF pattern.

Note On Cisco ASA 5500 series security appliances, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

Examples

The following example erases and reformats the file system:

```
hostname# erase flash:
```

Related Commands

Command	Description
delete	Removes all visible files, excluding hidden system files.
format	Erases all files (including hidden system files) and formats the file system.

esp

To specify parameters for esp and AH tunnels for IPSec Pass Thru inspection, use the **esp** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

{**esp** | **ah**} [**per-client-max** *num***] [timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num***] [timeout** *time*]

Syntax Description

esp	Specifies parameters for esp tunnel.
ah	Specifies parameters for AH tunnel.
per-client-max *num*	Specifies maximum tunnels from one client.
timeout *time*	Specifies idle timeout for the esp tunnel.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to permit UDP 500 traffic:

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

established

To permit return connections on ports that are based on an established connection, use the **established** command in global configuration mode. To disable the **established** feature, use the **no** form of this command.

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

Syntax Description

est_protocol	Specifies the IP protocol (UDP or TCP) to use for the established connection lookup.
dest_port	Specifies the destination port to use for the established connection lookup.
permitfrom	(Optional) Allows the return protocol connection(s) originating from the specified port.
permitto	(Optional) Allows the return protocol connections destined to the specified port.
port [*-port*]	(Optional) Specifies the (UDP or TCP) destination port(s) of the return connection.
protocol	(Optional) IP protocol (UDP or TCP) used by the return connection.
source_port	(Optional) Specifies the source port to use for the established connection lookup.

Defaults

The defaults are as follows:

- *dest_port*—0 (wildcard)
- *source_port*—0 (wildcard)

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keywords **to** and **from** were removed from the CLI. Use the keywords **permitto** and **permitfrom** instead.

Usage Guidelines

The **established** command lets you permit return access for outbound connections through the security appliance. This command works with an original connection that is outbound from a network and protected by the security appliance and a return connection that is inbound between the same two devices on an external host. The **established** command lets you specify the destination port that is used for

connection lookups. This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is unknown. The **permitto** and **permitfrom** keywords define the return inbound connection.

Caution We recommend that you always specify the **established** command with the **permitto** and **permitfrom** keywords. Using the **established** command without these keywords is a security risk because when connections are made to external systems, those system can make unrestricted connections to the internal host involved in the connection. This situation can be exploited for an attack of your internal systems.

Examples

The following set of examples shows potential security violations could occur if you do not use the **established** command correctly.

This example shows that if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
hostname(config)# established tcp 4000 0
```

You can specify the source and destination ports as **0** if the protocol does not specify which ports are used. Use wildcard ports (0) only when necessary.

```
hostname(config)# established tcp 0 0
```

Note To allow the **established** command to work properly, the client must listen on the port that is specified with the **permitto** keyword.

You can use the **established** command with the **nat 0** command (where there are no **global** commands).

Note You cannot use the **established** command with PAT.

The security appliance supports XDMCP with assistance from the **established** command.

Caution Using XWindows system applications through the security appliance may cause security risks.

XDMCP is on by default, but it does not complete the session unless you enter the **established** command as follows:

```
hostname(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

Entering the **established** command enables the internal XDMCP-equipped (UNIX or ReflectionX) hosts to access external XDMCP-equipped XWindows servers. UDP/177-based XDMCP negotiates a TCP-based XWindows session, and subsequent TCP back connections are permitted. Because the source port(s) of the return traffic is unknown, specify the *source_port* field as 0 (wildcard). The *dest_port* should be 6000 + *n*, where *n* represents the local display number. Use this UNIX command to change this value:

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connections is unknown. Only the destination port is static. The security appliance performs XDMCP fixups transparently. No configuration is required, but you must enter the **established** command to accommodate the TCP session.

The following example shows a connection between two hosts using protocol A destined for port B from source port C. To permit return connections through the security appliance and protocol D (protocol D can be different from protocol A), the source port(s) must correspond to port F and the destination port(s) must correspond to port E.

```
hostname(config)# established A B C permitto D E permitfrom D F
```

The following example shows how a connection is started by an internal host to an external host using TCP destination port 6060 and any source port. The security appliance permits return traffic between the hosts through TCP destination port 6061 and any TCP source port.

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

The following example shows how a connection is started by an internal host to an external host using UDP destination port 6060 and any source port. The security appliance permits return traffic between the hosts through TCP destination port 6061 and TCP source port 1024-65535.

```
hostname(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

The following example shows how a local host starts a TCP connection on port 9999 to a foreign host. The example allows packets from the foreign host on port 4242 back to local host on port 5454.

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

Related Commands

Command	Description
clear configure established	Removes all established commands.
show running-config established	Displays the allowed inbound connections that are based on established connections.

exceed-mss

To allow or drop packets whose data length exceeds the TCP maximum segment size set by the peer during a three-way handshake, use the **exceed-mss** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

Syntax Description

allow	Allows packets that exceed the MSS. This setting is the default.
drop	Drops packets that exceed the MSS.

Defaults

Packets are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)/8.0(4)	The default was changed from **drop** to **allow**.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **exceed-mss** command in tcp-map configuration mode to drop TCP packets whose data length exceed the TCP maximum segment size set by the peer during a three-way handshake.

Examples

The following example drops flows on port 21 if they are in excess of MSS:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss drop
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection advanced-options	Configures advanced connection features, including TCP normalization.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

exempt-list

To add an entry to the list of remote computer types that are exempt from posture validation, use the **exempt-list** command in nac-policy-nac-framework configuration mode. To remove an entry from the exemption list, use the **no** form of this command and name the operating system, and ACL, in the entry to be removed.

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

Syntax Description

acl-name	Name of the ACL present in the security appliance configuration. When specified, it must follow the **filter** keyword.
disable	Performs one of two functions, as follows: • If you enter it after the "os-name," the security appliance ignores the exemption, and applies NAC posture validation to the remote hosts that are running that operating system. • If you enter it after the *acl-name*, security appliance exempts the operating system, but does not assign the ACL to the associated traffic.
filter	Applies an ACL to filter the traffic if the computer's operating system matches the *os name*. The **filter**/*acl-name* pair is optional.
os	Exempts an operating system from posture validation.
os name	Operating system name. Quotation marks are required only if the name includes a space (for example, `"Windows XP"`).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	Command name changed from **vpn-nac-exempt** to **exempt-list**. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

When the command specifies an operating system, it does not overwrite the previously added entry to the exception list; enter the command once for each operating system and ACL you want to exempt.

The **no exempt-list** command removes all exemptions from the NAC Framework policy. Specifying an entry when issuing the **no** form of the command removes the entry from the exemption list.

To remove all entries from the exemption list associated with this NAC policy, use the **no** form of this command without specifying additional keywords.

Examples

The following example adds all hosts running Windows XP to the list of computers that are exempt from posture validation:

```
hostname(config-group-policy)# exempt-list os "Windows XP"
hostname(config-group-policy)
```

The following example exempts all hosts running Windows XP and applies the ACL acl-1 to traffic from those hosts:

```
hostname(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

The following example removes the same entry from the exemption list:

```
hostname(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

The following example removes all entries from the exemption list:

```
hostname(config-nac-policy-nac-framework)# no exempt-list
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
show vpn-session_summary.db	Displays the number IPSec, Cisco AnyConnect, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

exit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **exit** command in privileged or user EXEC modes, you log out from the security appliance. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **exit** command to exit global configuration mode, and then logout from the session:

```
hostname(config)# exit
hostname# exit

Logoff
```

The following example shows how to use the **exit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
hostname(config)# exit
hostname# disable
hostname>
```

Related Commands

Command	Description
quit	Exits a configuration mode or logs out from privileged or user EXEC modes.

expiry-time

To configure an expiration time for caching objects without revalidating them, use the **expiry-time** command in cache configuration mode. To remove the expiration time from the configuration and reset it to the default value, use the **no** form of this command.

expiry-time *time*

no expiry-time

Syntax Description

time	The amount of time in minutes that the security appliance caches objects without revalidating them.

Defaults

One minute.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cache configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The expiration time is the amount of time in minutes that the security appliance caches an object without revalidating it. Revalidation consists of rechecking the content.

Examples

The following example shows how to set an expiration time with a value of 13 minutes:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.

Command	Description
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

export

To specify the certificate to be exported to the client, use the **export** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

Syntax Description

certificate *trustpoint_name*	Specifies the certificate to be exported to the client.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **export** command in CTL provider configuration mode to specify the certificate to be exported to the client. The trustpoint name is defined by the **crypto ca trustpoint** command. The certificate will be added to the Certificate Trust List file composed by the CTL client.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.

Commands	Description
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

export webvpn customization

To export a customization object that customizes screens visible to Clientless SSL VPN users, use the **export webvpn customization** command from privileged EXEC mode.

export webvpn customization *name url*

Syntax Description

name	The name that identifies the customization object. Maximum 64 characters.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (maximum 255 characters).

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A customization object is an XML file that resides in cache memory, and customizes the screens visible to Clientless SSL VPN users, including logon and logout screens, the portal page, and available languages. When you export a customization object, an XML file containing XML tags is created at the URL you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the security appliance as a new customization object.

The content of Template is the same as the initial DfltCustomization object state.

You can export a customization object using the **export webvpn customization** command, make changes to the XML tags, and import the file as a new object using the **import webvpn customization** command.

Examples

The following example exports the default customization object (DfltCustomization) and creates the resulting XML file named dflt_custom:

```
hostname# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
```

```
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
hostname#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn translation-table

To export a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **export webvpn translation-table** command from privileged EXEC mode.

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

Syntax Description

language	Specifies the name of a previously-imported translation table. Enter the value in the manner expressed by your browser language options.
translation_domain	The functional area and associated messages. The usage guidelines section lists available translation domains.
url	Specifies the URL of the object.

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that is visible to remote users has its own translation domain and is specified by the *translation_domain* argument. The following table shows the translation domains and the functional areas translated.

Table 12-1 Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.

Translation Domain	Functional Areas Translated
banners	Banners displayed to remote users and messages when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the security appliance includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless users, the security appliance generates the **customization** and **url-list** translation domain templates dynamically and the template automatically reflects your changes to these functional areas.

Exporting a previously-imported translation table creates an XML file of the table at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn translation-table** command.

Download a template or translation table using the **export webvpn translation-table** command, make changes to the messages, and import the translation table using the **import webvpn translation-table** command.

Examples

The following example exports a template for the translation domain *customization*, which is used to translate the logon and logout pages, portal page, and all the messages customizable and visible to remote users establishing clientless SSL VPN connections. The security appliance creates the XML file with the name *Sales*:

```
hostname# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The next example exports a previously-imported translation table for the Chinese language named *zh*, an abbreviation compatible with the abbreviation specified for Chinese in the Internet Options of the Microsoft Internet Explorer browser. The security appliance creates the XML file with the name *Chinese*:

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

export webvpn url-list

To export a URL list to a remote location, use the **export webvpn url-list** command from privileged EXEC mode.

export webvpn url-list *name url*

Syntax Description

name	The name that identifies the URL list. Maximum 64 characters.
URL	Remote path to the source of the URL list. Maximum 255 characters.

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

No URL lists are present in WebVPN by default.

An object, Template, is available for downloading with the **export webvpn url-list** command. Template cannot be changed or deleted. The contents of Template can be edited and saved as a custom URL list, and imported with the **import webvpn url-list** command to add a custom URL list.

Exporting a previously-imported URL list creates an XML file of the list at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn url-list** command.

Examples

The following example exports a URL list, *servers*:

```
hostname# export webvpn url-list servers2 tftp://209.165.200.225
hostname#
```

Related Commands

Command	Description
import webvpn url-list	Imports a URL list.

revert webvpn url-list	Removes URL lists from cache memory.
show import webvpn url-list	Displays information about imported URL lists.

export webvpn webcontent

To export previously-imported content in flash memory that is visible to remote Clientless SSL VPN users, use the **export webvpn webcontent** command from privileged EXEC mode.

export webvpn webcontent <*source url*> <*destination url*>

Syntax Description

<*source url*>	The URL in the security appliance flash memory where the content resides. See Maximum 64 characters.
<*destination url*>	The URL to export to. Maximum 255 characters.

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Content exported with the **webcontent** option is content visible to remote Clientless users. This includes previously-imported help content visible on the Clientless portal and logos used by customization objects.

You can see a list of content available for export by entering a question mark (**?**) after the **export webvpn webcontent** command. For example:

```
hostname# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

Examples

The following example exports the file *logo.gif*, using tftp, to 209.165.200.225, as the filename *logo_copy.gif*:

```
hostname# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

Related Commands

Command	Description
import webvpn webcontent	Imports content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

failover

To enable failover, use the **failover** command in global configuration mode. To disable failover, use the **no** form of this command.

failover

no failover

Syntax Description

This command has no arguments or keywords.

Defaults

Failover is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was limited to enable or disable failover in the configuration (see the **failover active** command).

Usage Guidelines

Use the **no** form of this command to disable failover.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

The ASA 5505 device allows only Stateless Failover, and only while not acting as an Easy VPN hardware client.

Examples

The following example disables failover:

```
hostname(config)# no failover
hostname(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover active

To switch a standby security appliance or failover group to the active state, use the **failover active** command in privileged EXEC mode. To switch an active security appliance or failover group to standby, use the **no** form of this command.

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

Syntax Description

group *group_id*	(Optional) Specifies the failover group to make active.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include failover groups.

Usage Guidelines

Use the **failover active** command to initiate a failover switch from the standby unit, or use the **no failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit offline for maintenance. If you are not using stateful failover, all active connections are dropped and must be reestablished by the clients after the failover occurs.

Switching for a failover group is available only for Active/Active failover. If you enter the **failover active** command on an Active/Active failover unit without specifying a failover group, all groups on the unit become active.

Examples

The following example switches the standby group 1 to active:

```
hostname# failover active group 1
```

Related Commands

Command	Description
failover reset	Moves a security appliance from a failed state to standby.

failover exec

To execute a command on a specific unit in a failover pair, use the **failover exec** command in privileged EXEC or global configuration mode.

failover exec {**active** | **standby** | **mate**} *cmd_string*

Syntax Description

active	Specifies that the command is executed on the active unit or failover group in the failover pair. Configuration commands entered on the active unit or failover group are replicated to the standby unit or failover group.
cmd_string	The command to be executed. Show, configuration, and exec commands are supported.
mate	Specifies that the command is executed on the failover peer.
standby	Specifies that the command is executed on the standby unit or failover group in the failover pair. Configuration commands executed on the standby unit or failover group are not replicated to the active unit or failover group.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **failover exec** command to send commands to a specific unit in a failover pair.

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the **failover exec** command to enter configuration commands on the correct unit, no matter which unit you are logged-in to. For example, if you are logged-in to the standby unit, you can use the **failover exec active** command to send configuration changes to the active unit. Those changes are then replicated to the standby unit. Do not use the **failover exec** command to send configuration commands to the standby unit or context; those configuration changes are not replicated to the active unit and the two configurations will no longer be synchronized.

Output from configuration, exec, and **show** commands is displayed in the current terminal session, so you can use the **failover exec** command to issue **show** commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

Command Modes

The **failover exec** command maintains a command mode state that is separate from the command mode of your terminal session. By default, the **failover exec** command mode is global configuration mode for the specified device. You can change that command mode by sending the appropriate command (such as the **interface** command) using the **failover exec** command.

Changing **failover exec** command modes for the specified device does not change the command mode for the session you are using to access the device. For example, if you are logged-in to the active unit of a failover pair, and you issue the following command from global configuration mode, you will remain in global configuration mode but any commands sent using the **failover exec** command will be executed in interface configuration mode:

```
hostname(config)# failover exec interface GigabitEthernet0/1
hostname(config)#
```

Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command. For example, if you are in interface configuration mode on the active unit, and you have not changed the **failover exec** command mode, the following command would be executed in global configuration mode:

```
hostname(config-if)# failover exec active router ospf 100
hostname(config-if)#
```

Use the **show failover exec** command to display the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Security Considerations

The **failover exec** command uses the failover link to send commands to and receive the output of the command execution from the peer unit. You should use the **failover key** command to encrypt the failover link to prevent eavesdropping or man-in-the-middle attacks.

Limitations

- If you upgrade one unit using the zero-downtime upgrade procedure and not the other, both units must be running software that supports the **failover exec** command for the command to work.
- Command completion and context help is not available for the commands in the *cmd_string* argument.
- In multiple context mode, you can only send commands to the peer context on the peer unit. To send commands to a different context, you must first change to that context on the unit you are logged-in to.
- You cannot use the following commands with the **failover exec** command:
  - **changeto**
  - **debug** (**undebug**)
- If the standby unit is in the failed state, it can still receive commands from the **failover exe**c command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot use the **failover exec** command to switch from privileged EXEC mode to global configuration mode on the failover peer. For example, if the current unit is in privileged EXEC mode, and you enter **failover exec mate configure terminal**, the **show failover exec mate** output

will show that the failover exec session is in global configuration mode. However, entering configuration commands for the peer unit using **failover exec** will fail until you enter global configuration mode on the current unit.

- You cannot enter recursive failover exec commands, such as **failover exec mate failover exec mate** *command.*
- Commands that require user input or confirmation must use the **/nonconfirm** option.

Examples

The following example shows how to use the **failover exec** command to display failover information on the active unit. The unit on which the command is executed is the active unit, so the command is executed locally.

```
hostname(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
hostname(config)#
```

The following example uses the **failover exec** command to display the failover status of the peer unit. The command is executed on the the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show failover
```

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

The following example uses the **failover exec** command to display the failover configuration of the failover peer. The command is executed on the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

The following example uses the **failover exec** command to create a context on the active unit from the standby unit. The command is replicated from the active unit back to the standby unit. Note the two "Creating context…" messages. One is from the **failover exec** command output from the peer unit when the context is created, and the other is from the local unit when the replicated command creates the context locally.

```
hostname(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

hostname(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

hostname(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

The following example shows the warning that is returned when you use the **failover exec** command to send configuration commands to a failover peer in the standby state:

```
hostname# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

       **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
hostname(config)#
```

The following example uses the **failover exec** command to send the **show interface** command to the standby unit:

```
hostname(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
```

```
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

The following example shows the error message returned when issuing an illegal command to the peer unit:

```
hostname# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

The following example shows the error message that is returned when you use the **failover exec** command when failover is disabled:

```
hostname(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

Command	Description
debug fover	Displays failover-related debug messages.
debug xml	Displays debug messages for the XML parser used by the **failover exec** command.
show failover exec	Displays the **failover exec** command mode.

failover group

To configure an Active/Active failover group, use the **failover group** command in global configuration mode. To remove a failover group, use the **no** form of this command.

failover group *num*

no failover group *num*

Syntax Description

num	Failover group number. Valid values are 1 or 2.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can define a maximum of 2 failover groups. The **failover group** command can only be added to the system context of devices configured for multiple context mode. You can create and remove failover groups only when failover is disabled.

Entering this command puts you in the failover group command mode. The **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, **mac address**, and **polltime interface** commands are available in the failover group configuration mode. Use the **exit** command to return to global configuration mode.

Note The **failover polltime interface**, **failover interface-policy**, **failover replication http**, and **failover mac address** commands have no effect in Active/Active failover configurations. They are overridden by the following failover group configuration mode commands: **polltime interface**, **interface-policy**, **replication http**, and **mac address**.

When removing failover groups, you must remove failover group 1 last. Failover group 1 always contains the admin context. Any context not assigned to a failover group defaults to failover group 1. You cannot remove a failover group that has contexts explicitly assigned to it.

Note If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address using the **mac address** command.

Examples

The following partial example shows a possible configuration for two failover groups:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
asr-group	Specifies an asymmetrical routing interface group ID.
interface-policy	Specifies the failover policy when monitoring detects interface failures.
join-failover-group	Assigns a context to a failover group.
mac address	Defines virtual mac addresses for the contexts within a failover group.
polltime interface	Specifies the amount of time between hello messages sent to monitored interfaces.
preempt	Specifies that a unit with a higher priority becomes the active unit after a reboot.
primary	Gives the primary unit higher priority for a failover group.
replication http	Specifies HTTP session replication for the selected failover group.
secondary	Gives the secondary unit higher priority for a failover group.

failover interface ip

To specify the IP address and mask for the failover interface and the Stateful Failover interface, use the **failover interface ip** command in global configuration mode. To remove the IP address, use the **no** form of this command.

failover interface ip *if_name ip_address mask* **standby** *ip_address*

no failover interface ip *if_name ip_address mask* **standby** *ip_address*

Syntax Description

if_name	Interface name for the failover or stateful failover interface.
ip_address mask	Specifies the IP address and mask for the failover or stateful failover interface on the primary module.
standby *ip_address*	Specifies the IP address used by the secondary module to communicate with the primary module.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Failover and stateful failover interfaces are functions of Layer 3, even when the security appliance is operating in transparent firewall mode, and are global to the system.

In multiple context mode, you configure failover in the system context (except for the **monitor-interface** command).

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Examples

The following example shows how to specify the IP address and mask for the failover interface:

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover lan interface	Specifies the interface used for failover communication.
failover link	Specifies the interface used for Stateful Failover.
monitor-interface	Monitors the health of the specified interface.
show running-config failover	Displays the **failover** commands in the running configuration.

failover interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **failover interface-policy** command in global configuration mode. To restore the default, use the **no** form of this command.

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces when used as a number.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

The defaults are as follows:

- *num* is 1.
- Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other security appliance is functioning properly, the security appliance marks itself as failed and a failover might occur (if the active security appliance is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the interface policy for each failover group with the **interface-policy** command in failover group configuration mode.

Examples

The following examples show two ways to specify the failover policy:

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit and interface poll times.
failover reset	Restores a failed unit to an unfailed state.
monitor-interface	Specifies the interfaces being monitored for failover.
show failover	Displays information about the failover state of the unit.

failover key

To specify the key for encrypted and authenticated communication between units in a failover pair, use the **failover key** command in global configuration mode. To remove the key, use the **no** form of this command.

failover key {*secret* | **hex** *key*}

no failover key

Syntax Description

hex *key*	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0-9, a-f).
secret	Specifies an alphanumeric shared secret. The secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified from **failover lan key** to **failover key**.
7.0(4)	This command was modified to include the **hex** *key* keyword and argument.

Usage Guidelines

To encrypt and authenticate failover communications between the units, you must configure both units with a shared secret or hexadecimal key. If you do not specify a failover key, failover communication is transmitted in the clear.

Note On the PIX security appliance platform, if you are using the dedicated serial failover cable to connect the units, then communication over the failover link is not encrypted even if a failover key is configured. The failover key only encrypts LAN-based failover communication.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels.

Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example shows how to specify a shared secret for securing failover communication between units in a failover pair:

```
hostname(config)# failover key abcdefg
```

The following example shows how to specify a hexadecimal key for securing failover communication between two units in a failover pair:

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.

failover lan enable

To enable lan-based failover on the PIX security appliance, use the **failover lan enable** command in global configuration mode. To disable LAN-based failover, use the **no** form of this command.

failover lan enable

no failover lan enable

Syntax Description

This command has no arguments or keywords.

Defaults

Not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When LAN-based failover is disabled using the **no** form of this command, cable-based failover is used if the failover cable is installed. This command is available on the PIX security appliance only.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example enables LAN-based failover:

```
hostname(config)# failover lan enable
```

Related Commands

Command	Description
failover lan interface	Specifies the interface used for failover communication.
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover lan interface

To specify the interface used for failover communication, use the **failover lan interface** command in global configuration mode. To remove the failover interface, use the **no** form of this command.

failover lan interface *if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}]

Syntax Description

if_name	Specifies the name of the security appliance interface dedicated to failover.
phy_if	Specifies the physical interface.
sub_if	(Optional) Specifies a subinterface number.
vlan_if	Used on the ASA 5505 adaptive security appliance to specify a VLAN interface as the failover link.

Defaults

Not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include the *phy_if* argument.
7.2(1)	This command was modified to include the *vlan_if* argument.

Usage Guidelines

LAN failover requires a dedicated interface for passing failover traffic. However you can also use the LAN failover interface for the Stateful Failover link.

Note If you use the same interface for both LAN failover and Stateful Failover, the interface needs enough capacity to handle both the LAN-based failover and Stateful Failover traffic.

You can use any unused Ethernet interface on the device as the failover interface. You cannot specify an interface that is currently configured with a name. The failover interface is not configured as a normal networking interface; it exists only for failover communications. This interface should only be used for the failover link (and optionally for the state link). You can connect the LAN-based failover link by using a dedicated switch with no hosts or routers on the link or by using a crossover Ethernet cable to link the units directly.

Note When using VLANs, use a dedicated VLAN for the failover link. Sharing the failover link VLAN with any other VLANs can cause intermittent traffic problems and ping and ARP failures. If you use a switch to connect the failover link, use dedicated interfaces on the switch and security appliance for the failover link; do not share the interface with subinterfaces carrying regular network traffic.

On systems running in multiple context mode, the failover link resides in the system context. This interface and the state link, if used, are the only interfaces that you can configure in the system context. All other interfaces are allocated to and configured from within security contexts.

Note The IP address and MAC address for the failover link do not change at failover.

The **no** form of this command also clears the failover interface IP address configuration.

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example configures the failover LAN interface on a PIX 500 series security appliance:

```
hostname(config)# failover lan interface folink Ethernet4
```

The following example configures the failover LAN interface using a subinterface on an ASA 5500 series adaptive security appliance (except for the ASA 5505 adaptive security appliance):

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

The following example configures the failover LAN interface on the ASA 5505 adaptive security appliance:

```
hostname(config)# failover lan interface folink Vlan6
```

Related Commands

Command	Description
failover lan enable	Enables LAN-based failover on the PIX security appliance.
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
failover link	Specifies the Stateful Failover interface.

failover lan unit

To configure the security appliance as either the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

Syntax Description

primary	Specifies the security appliance as a primary unit.
secondary	Specifies the security appliance as a secondary unit.

Defaults

Secondary.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For Active/Standby failover, the primary and secondary designation for the failover unit refers to which unit becomes active at boot time. The primary unit becomes the active unit at boot time when the following occurs:

- The primary and secondary unit both complete their boot sequence within the first failover poll check.
- The primary unit boots before the secondary unit.

If the secondary unit is already active when the primary unit boots, the primary unit does not take control; it becomes the standby unit. In this case, you need to issue the **no failover active** command on the secondary (active) unit to force the primary unit back to active status.

For Active/Active failover, each failover group is assigned a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover group become active at startup when both units start simultaneously (within the failover polling period).

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Examples

The following example sets the security appliance as the primary unit in LAN-based failover:

```
hostname(config)# failover lan unit primary
```

Related Commands

Command	Description
failover lan enable	Enables LAN-based failover on the PIX security appliance.
failover lan interface	Specifies the interface used for failover communication.

failover link

To specify the Stateful Failover interface, use the **failover link** command in global configuration mode. To remove the Stateful Failover interface, use the **no** form of this command.

failover link *if_name* [*phy_if*]

no failover link

Syntax Description

if_name	Specifies the name of the security appliance interface dedicated to Stateful Failover.
phy_if	(Optional) Specifies the physical or logical interface port. If the Stateful Failover interface is sharing the interface assigned for failover communication or sharing a standard firewall interface, then this argument is not required.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to include the *phy_if* argument.
7.0(4)	This command was modified to accept standard firewall interfaces.

Usage Guidelines

This command is not available on the ASA 5505 series adaptive security appliance, which does not support Stateful Failover.

The physical or logical interface argument is required when not sharing the failover communication or a standard firewall interface.

The **failover link** command enables Stateful Failover. Enter the **no failover link** command to disable Stateful Failover. If you are using a dedicated Stateful Failover interface, the **no failover link** command also clears the Stateful Failover interface IP address configuration.

To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- You can use a dedicated Ethernet interface for the Stateful Failover link.
- If you are using LAN-based failover, you can share the failover link.

- You can share a regular data interface, such as the inside interface. However, this option is not recommended.

If you are using a dedicated Ethernet interface for the Stateful Failover link, you can use either a switch or a crossover cable to directly connect the units. If you use a switch, no other hosts or routers should be on this link.

Note Enable the PortFast option on Cisco switch ports that connect directly to the security appliance.

If you are using the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.

If you use a data interface as the Stateful Failover link, you will receive the following warning when you specify that interface as the Stateful Failover link:

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

Sharing a data interface with the Stateful Failover interface can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment.

Note Using a data interface as the Stateful Failover interface is only supported in single context, routed mode.

In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.

Note The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example shows how to specify a dedicated interface as the Stateful Failover interface. The interface in the example does not have an existing configuration.

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

Related Commands

Command	Description
failover interface ip	Configures the IP address of the **failover** command and stateful failover interface.
failover lan interface	Specifies the interface used for failover communication.

failover mac address

To specify the failover virtual MAC address for a physical interface, use the **failover mac address** command in global configuration mode. To remove the virtual MAC address, use the **no** form of this command.

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

Syntax Description

phy_if	The physical name of the interface to set the MAC address.
active_mac	The MAC address assigned to the specified interface the active security appliance. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
standby_mac	The MAC address assigned to the specified interface of the standby security appliance. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Defaults

Not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **failover mac address** command lets you configure virtual MAC addresses for an Active/Standby failover pair. If virtual MAC addresses are not defined, then when each failover unit boots it uses the burned-in MAC addresses for its interfaces and exchanges those addresses with its failover peer. The MAC addresses for the interfaces on the primary unit are used for the interfaces on the active unit.

However, if both units are not brought online at the same time and the secondary unit boots first and becomes active, it uses the burned-in MAC addresses for its own interfaces. When the primary unit comes online, the secondary unit will obtain the MAC addresses from the primary unit. This change can disrupt network traffic. Configuring virtual MAC addresses for the interfaces ensures that the secondary unit uses the correct MAC address when it is the active unit, even if it comes online before the primary unit.

The **failover mac address** command is unnecessary (and therefore cannot be used) on an interface configured for LAN-based failover because the **failover lan interface** command does not change the IP and MAC addresses when failover occurs. This command has no effect when the security appliance is configured for Active/Active failover.

When adding the **failover mac address** command to your configuration, it is best to configure the virtual MAC address, save the configuration to Flash memory, and then reload the failover pair. If the virtual MAC address is added when there are active connections, then those connections stop. Also, you must write the complete configuration, including the **failover mac address** command, to the Flash memory of the secondary security appliance for the virtual MAC addressing to take effect.

If the **failover mac address** is specified in the configuration of the primary unit, it should also be specified in the bootstrap configuration of the secondary unit.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the virtual MAC address for each interface in a failover group with the **mac address** command in failover group configuration mode.

Examples

The following example configures the active and standby MAC addresses for the interface named intf2:

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

Related Commands

Command	Description
show interface	Displays interface status, configuration, and statistics.

failover polltime

To specify the failover unit poll and hold times, use the **failover polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values are from 3 to 45 seconds or from 800 to 999 milliseconds if the optional **msec** keyword is used.
msec	(Optional) Specifies that the given time is in milliseconds.
poll_time	Amount of time between hello messages. Valid values are from 1 to 15 seconds or from 200 to 999 milliseconds if the optional **msec** keyword is used.
unit	(Optional) Indicates that the command is used for unit poll and hold times. Adding this keyword to the command does not have any affect on the command, but it can make it easier to differentiate this command from the **failover polltime interface** commands in the configuration.

Defaults

The default values on the PIX security appliance are as follows:

- The *poll_time* is 15 seconds.
- The **holdtime** *time* is 45 seconds.

The default values on the ASA security appliance are as follows:

- The *poll_time* is 1 second.
- The **holdtime** *time* is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and now includes **unit** and **holdtime** keywords.
7.2(1)	The **msec** keyword was added to the **holdtime** keyword. The **polltime** minimum value was reduced to 200 milliseconds from 500 milliseconds. The **holdtime** minimum value was reduced to 800 milliseconds from 3 seconds.

Usage Guidelines

You cannot enter a **holdtime** value that is less than 3 times the unit poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switch overs when the network is temporarily congested.

If a unit does not hear hello packet on the failover communication interface or cable for one polling period, additional testing occurs through the remaining interfaces. If there is still no response from the peer unit during the hold time, the unit is considered failed and, if the failed unit is the active unit, the standby unit takes over as the active unit.

You can include both **failover polltime** [**unit**] and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example changes the unit poll time frequency to 3 seconds:

```
hostname(config)# failover polltime 3
```

The following example configures the security appliance to send a hello packet every 200 milliseconds and to fail over in 800 milliseconds if no hello packets are received on the failover interface within that time. The optional **unit** keyword is included in the command.

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

Related Commands

Command	Description
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.
polltime interface	Specifies the interface poll and hold times for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover polltime interface

To specify the data interface poll and hold times in an Active/Standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 seconds.
interface *time*	Specifies the poll time for interface monitoring. Valid values range from 1 to 15 seconds. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Defaults

The default values are as follows:

- The poll *time* is 5 seconds.
- The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from the **failover poll** command to the **failover polltime** command and includes **unit**, **interface**, and **holdtime** keywords.
7.2(1)	The optional **holdtime** *time* and the ability to specify the poll time in milliseconds was added.

Usage Guidelines

Use the **failover polltime interface** command to change the frequency that hello packets are sent out on data interfaces. This command is available for Active/Standby failover only. For Active/Active failover, use the **polltime interface** command in failover group configuration mode instead of the **failover polltime interface** command.

You cannot enter a **holdtime** value that is less than 5 times the unit poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested. Interface testing begins when a hello packet is not heard on the interface for over half the hold time.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example sets the interface poll time frequency to 15 seconds:

```
hostname(config)# failover polltime interface 15
```

The following example sets the interface poll time frequency to 500 milliseconds and the hold time to 5 seconds:

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit failover poll and hold times.
polltime interface	Specifies the interface polltime for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover reload-standby

To force the standby unit to reboot, use the **failover reload-standby** command in privileged EXEC mode.

failover reload-standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command when your failover units do not synchronize. The standby unit restarts and resynchronizes to the active unit after it finishes booting.

Examples

The following example shows how to use the **failover reload-standby** command on the active unit to force the standby unit to reboot:

```
hostname# failover reload-standby
```

Related Commands

Command	Description
write standby	Writes the running configuration to the memory on the standby unit.

failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command in global configuration mode. To disable HTTP connection replication, use the **no** form of this command.

failover replication http

no failover replication http

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was changed from **failover replicate http** to **failover replication http**.

Usage Guidelines

By default, the security appliance does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **failover replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

In Active/Active failover configurations, you control HTTP session replication per failover group using the **replication http** command in failover group configuration mode.

Examples

The following example shows how to enable HTTP connection replication:

```
hostname(config)# failover replication http
```

Related Commands

Command	Description
replication http	Enables HTTP session replication for a specific failover group.
show running-config failover	Displays the **failover** commands in the running configuration.

failover reset

To restore a failed security appliance to an unfailed state, use the **failover reset** command in privileged EXEC mode.

failover reset [**group** *group_id*]

Syntax Description

group	(Optional) Specifies a failover group. The **group** keyword applies to Active/Active failover only.
group_id	Failover group number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to allow the optional failover group ID.

Usage Guidelines

The **failover reset** command allows you to change the failed unit or group to an unfailed state. The **failover reset** command can be entered on either unit, but we recommend that you always enter the command on the active unit. Entering the **failover reset** command at the active unit will "unfail" the standby unit.

You can display the failover status of the unit with the **show failover** or **show failover state** commands.

There is no **no** version of this command.

In Active/Active failover, entering **failover reset** resets the whole unit. Specifying a failover group with the command resets only the specified group.

Examples

The following example shows how to change a failed unit to an unfailed state:

```
hostname# failover reset
```

Related Commands

Command	Description
failover interface-policy	Specifies the policy for failover when monitoring detects interface failures.
show failover	Displays information about the failover status of the unit.

failover timeout

To specify the failover reconnect timeout value for asymmetrically routed sessions, use the **failover timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

Syntax Description

hh	Specifies the number of hours in the timeout value. Valid values range from -1 to 1193. By default, this value is set to 0. Setting this value to -1 disables the timeout, allowing connections to reconnect after any amount of time. Setting this value to 0, without specifying any of the other timeout values, sets the command back to the default value, which prevents connections from reconnecting. Entering **no failover timeout** command also sets this value to the default (0). **Note** When set to the default value, this command does not appear in the running configuration.
mm	(Optional) Specifies the number of minutes in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.
ss	(Optional) Specifies the number of seconds in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.

Defaults

By default, *hh*, *mm*, and *ss* are 0, which prevents connections from reconnecting.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to appear in the command listing.

Usage Guidelines

This command is used in conjunction with the **static** command with the **nailed** option. The **nailed** option allows connections to be reestablished in a specified amount of time after bootup or a system goes active. The **failover timeout** command specifies that amount of time. If not configured, the connections cannot be reestablished. The **failover timeout** command does not affect the **asr-group** command.

Note Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection.

Enter the **no** form of this command restores the default value. Entering **failover timeout 0** also restores the default value. When set to the default value, this command does not appear in the running configuration.

Examples

The following example switches the standby group 1 to active:

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

Related Commands

Command	Description
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

file-bookmarks

To customize the File Bookmarks title or the File Bookmarks links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **file-bookmarks** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or CSS parameters (maximum 256 characters).

Defaults

The default link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “File Folder Bookmarks”.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the W3C website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the File Bookmarks title to “Corporate File Bookmarks”:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

file-browsing

To enable or disable CIFS/FTP file browsing for file servers or shares, use the **file-browsing** command in dap webvpn configuration mode.

file-browsing enable | disable

enable | disable	Enables or disables the ability to browse for file servers or shares.

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The following usage notes apply to file browsing:

- File browsing does not support internationalization.
- Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS.

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the security appliance applies that value and enforces it. For example, when you disable file browsing in dap webvpn mode, the security appliance looks no further for a value. When you instead set no value for the **file-browsing** command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file browsing for the DAP record called Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-browsing enable
hostname(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

file-encoding

To specify the character encoding for pages from Common Internet File System servers, use the **file-encoding** command in webvpn configuration mode. To remove the values of the file-encoding attribute use the **no** form of this command.

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper-case to lower-case in the security appliance configuration.
server-ip-addr	IP address, in dotted decimal notation, of the CIFS server for which you want to specify character encoding.
server-name	Name of the CIFS server for which you want to specify character encoding. The security appliance retains the case you specify, although it ignores the case when matching the name to a server.

Defaults

Pages from all CIFS servers that do not have explicit file-encoding entries in the WebVPN configuration inherit the character encoding value from the character-encoding attribute.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Enter file-encoding entries for all CIFS servers that require character encodings that differ from the value of the webvpn character-encoding attribute.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character-encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a

value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

Examples

The following example sets the file-encoding attribute of the CIFS server named “CISCO-server-jp” to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

The following example sets the file-encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias “CP860”) characters:

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

Related Commands

Command	Description
character-encoding	Specifies the global character encoding used in all WebVPN portal pages except for pages from servers specified in file-encoding entries in the WebVPN configuration.
show running-config [all] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debug messages about the Common Internet File System.

file-entry

To enable or disable the ability of a user to enter file server names to access, use the **file-entry** command in dap webvpn configuration mode.

file-entry enable | disable

enable | disable	Enables or disables the ability to enter file server names to access.

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the Connection Profile (tunnel group)
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or Connection Profile.

When you enable or disable an attribute for a DAP record, the security appliance applies that value and enforces it. For example, when you disable file entry in dap webvpn mode, the security appliance looks no further for a value. When you instead set no value for the **file-entry** command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file entry for the DAP record called Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-entry enable
```

```
hostname(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-browsing	Enables or disables the ability to browse for file servers or shares.

filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, including a null value created by issuing the **filter none** command, use the **no** form of this command.

filter {**value** *ACLname* | **none**}

no filter

Syntax Description

none	Indicates that there is no **webvpntype** access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *ACLname*	Provides the name of the previously configured access list.

Defaults

WebVPN access lists do not apply until you use the **filter** command to specify them.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **no** option allows inheritance of a value from another group policy. To prevent inheriting filter values, use the **filter value none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **filter** command to apply those ACLs for WebVPN traffic.

WebVPN does not use ACLs defined in the **vpn-filter** command.

Examples

The following example shows how to set a filter that invokes an access list named *acl_in* for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

filter activex

To remove ActiveX objects in HTTP traffic passing through the security appliance, use the **filter activex** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The **http** or **url** literal can be used for port 21. The range of values permitted is 0 to 65535. For a listing of the well-known ports and their literal values, see
-port	(Optional) Specifies a port range.
except	Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

ActiveX objects may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can disable ActiveX objects with the **filter activex** command.

ActiveX controls, formerly known as OLE or OCX controls, are components you can insert in a web page or other application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information. As a technology, ActiveX creates many potential problems for network clients including causing workstations to fail, introducing network security problems, or being used to attack servers.

The **filter activex** command command blocks the HTML <object> commands by commenting them out within the HTML web page. ActiveX filtering of HTML files is performed by selectively replacing the <APPLET> and </APPLET> and <OBJECT CLASSID> and </OBJECT> tags with comments. Filtering of nested tags is supported by converting top-level tags to comments.

Caution The <object> tag is also used for Java applets, image files, and multimedia objects, which will also be blocked by this command.

If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the security appliance cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command or for WebVPN traffic.

Examples

The following example specifies that Activex objects are blocked on all outbound connections:

```
hostname(config)# filter activex 80 0 0 0 0
```

This command specifies that the ActiveX object blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

Related Commands\

Commands	Description
filter url	Directs traffic to a URL filtering server.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies anN2H2 or Websense server for use with the **filter** command.

filter ftp

To identify the FTP traffic to be filtered by a Websense or N2H2 server, use the **filter ftp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The **ftp** literal can be used for port 80.
-port	(Optional) Specifies a port range.
except	Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back on line.
interact-block	(Optional) Prevents users from connecting to the FTP server through an interactive FTP program.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **filter ftp** command lets you identify the FTP traffic to be filtered by a Websense or N2H2 server.

After enabling this feature, when a user issues an FTP GET request to a server, the security appliance sends the request to the FTP server and to the Websense or N2H2 server at the same time. If the Websense or N2H2 server permits the connection, the security appliance allows the successful FTP return code to reach the user unchanged. For example, a successful return code is "250: CWD command successful."

If the Websense or N2H2 server denies the connection, the security appliance alters the FTP return code to show that the connection was denied. For example, the security appliance would change code 250 to "550 Requested file is prohibited by URL filtering policy." Websense only filters FTP GET commands and not PUT commands).

Use the **interactive-block** option to prevent interactive FTP sessions that do not provide the entire directory path. An interactive FTP client allows the user to change directories without typing the entire path. For example, the user might enter **cd ./files** instead of **cd /public/files**. You must identify and enable the URL filtering server before using these commands.

Examples

The following example shows how to enable FTP filtering:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter https	Identifies the HTTPS traffic to be filtered by a Websense sor N2H2 erver.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter https

To identify the HTTPS traffic to be filtered by a N2H2 or Websense server, use the **filter https** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter https <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 443, but other values are accepted. The **https** literal can be used for port 443.
-port	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 443 traffic until the N2H2 or Websense server is back on line.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance supports filtering of HTTPS and FTP sites using an external Websense or N2H2 filtering server.

HTTPS filtering works by preventing the completion of SSL connection negotiation if the site is not allowed. The browser displays an error message such as “The Page or the content cannot be displayed.”

Because HTTPS content is encrypted, the security appliance sends the URL lookup without directory and filename information.

Examples

The following example filters all outbound HTTPS connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter java

To remove Java applets from HTTP traffic passing through the security appliance, use the **filter java** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter java {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80.
port-port	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Java applets may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can remove Java applets with the **filter java** command.

The **filter java** command filters out Java applets that return to the security appliance from an outbound connection. The user still receives the HTML page, but the web page source for the applet is commented out so that the applet cannot execute. The **filter java** command does not filter WebVPN traffic.

If the applet or /applet HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the security appliance cannot block the tag. If Java applets are known to be in <object> tags, use the **filter activex** command to remove them.

Examples

The following example specifies that Java applets are blocked on all outbound connections:

```
hostname(config)# filter java 80 0 0 0 0
```

This command specifies that the Java applet blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

The following example blocks downloading of Java applets to a host on a protected network:

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

This command prevents host 192.168.3.3 from downloading Java applets.

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter url

To direct traffic to a URL filtering server, use the **filter url** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

Syntax Description

allow	When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back on line.
cgi_truncate	When a URL has a parameter list starting with a question mark (?), such as a CGI script, truncate the URL sent to the filtering server by removing all characters after and including the question mark.
except	Creates an exception to a previous **filter** condition.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
http	Specifies port 80. You can enter **http** or **www** instead of 80 to specify port 80.)
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
longurl-deny	Denies the URL request if the URL is over the URL buffer size limit or the URL buffer is not available.
longurl-truncate	Sends only the originating hostname or IP address to the N2H2 or Websense server if the URL is over the URL buffer limit.
mask	Any mask.
-port	(Optional) The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80. Adding a second port after a hyphen optionally identifies a range of ports.
proxy-block	Prevents users from connecting to an HTTP proxy server.
url	Filter URLs from data moving through the security appliance.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **filter url** command lets you prevent outbound users from accessing World Wide Web URLs that you designate using the N2H2 or Websense filtering application.

Note The **url-server** command must be configured before issuing the **filter url** command.

The **allow** option to the **filter url** command determines how the security appliance behaves if the N2H2 or Websense server goes off line. If you use the **allow** option with the **filter url** command and the N2H2 or Websense server goes offline, port 80 traffic passes through the security appliance without filtering. Used without the **allow** option and with the server off line, the security appliance stops outbound port 80 (Web) traffic until the server is back on line, or if another URL server is available, passes control to the next URL server.

Note With the **allow** option set, the security appliance now passes control to an alternate server if the N2H2 or Websense server goes off line.

The N2H2 or Websense server works with the security appliance to deny users from access to websites based on the company security policy.

Using the Filtering Server

Websense protocol Version 4 enables group and username authentication between a host and a security appliance. The security appliance performs a username lookup, and then Websense server handles URL filtering and username logging.

The N2H2 server must be a Windows workstation (2000, NT, or XP), running an IFP Server, with a recommended minimum of 512 MB of RAM. Also, the long URL support for the N2H2 service is capped at 3 KB, less than the cap for Websense.

Websense protocol Version 4 contains the following enhancements:

- URL filtering allows the security appliance to check outgoing URL requests against the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.
- Username lookup enables the security appliance to use the user authentication table to map the host's IP address to the username.

Information on Websense is available at the following website:

http://www.websense.com/

Configuration Procedure

Follow these steps to filter URLs:

Step 1 Designate an N2H2 or Websense server with the appropriate vendor-specific form of the **url-server** command.

Step 2 Enable filtering with the **filter** command.

Step 3 If needed, improve throughput with the **url-cache** command. However, this command does not update Websense logs, which may affect Websense accounting reports. Accumulate Websense run logs before using the **url-cache** command.

Step 4 Use the **show url-cache statistics** and the **show perfmon** commands to view run information.

Working with Long URLs

Filtering URLs up to 4 KB is supported for the Websense filtering server, and up to 3 KB for the N2H2 filtering server.

Use the **longurl-truncate** and **cgi-truncate** options to allow handling of URL requests longer than the maximum permitted size.

If a URL is longer than the maximum, and you do not enable the **longurl-truncate** or **longurl-deny** options, the security appliance drops the packet.

The **longurl-truncate** option causes the security appliance to send only the hostname or IP address portion of the URL for evaluation to the filtering server when the URL is longer than the maximum length permitted. Use the **longurl-deny** option to deny outbound URL traffic if the URL is longer than the maximum permitted.

Use the **cgi-truncate** option to truncate CGI URLs to include only the CGI script location and the script name without any parameters. Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request including the parameter list can use up memory resources and affect security appliance performance.

Buffering HTTP Responses

By default, when a user issues a request to connect to a specific website, the security appliance sends the request to the web server and to the filtering server at the same time. If the filtering server does not respond before the web content server, the response from the web server is dropped. This delays the web server response from the point of view of the web client.

By enabling the HTTP response buffer, replies from web content servers are buffered and the responses will be forwarded to the requesting user if the filtering server allows the connection. This prevents the delay that may otherwise occur.

To enable the HTTP response buffer, enter the following command:

```
url-block block block-buffer-limit
```

Replace *block-buffer* with the maximum number of blocks that will be buffered. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks that can be buffered at one time.

Examples

The following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

The following example blocks all outbound HTTP connections destined to a proxy server that listens on port 8080:

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

fips enable

To enable policy-checking to enforce FIPS compliance on the system or module, use the **fips enable** commandin global configuration mode. To disable policy-checkin, use the **no** form of this command.

fips enable

no fips enable

Syntax Description

enable	Enables or disables policy-checking to enforce FIPS compliance.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

To run in a FIPS-compliant mode of operation, you must apply both the **fips enable** command and the proper configuration specified in the Security Policy. The internal API allows the device to migrate towards enforcing proper configuration at run-time.

When “fips enable” is present in the startup-configuration, FIPS POST will run and print the following console message:

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
```

```
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

Examples

The following shows policy-checking to enforce FIPS compliance on the system:

```
sw8-ASA(config)# fips enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

fips self-test poweron

To execute power-on self-tests, use the **fips self-test powereon** commandin privileged EXEC mode.

fips self-test poweron

Syntax Description

poweron	Executes Power-On Self-Tests.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

Executing this command causes the device to run all self-tests required for FIPS 140-2 compliance. Tests are compreised of: cryptographic algorithm test, software integrity test and critical functions test.

Examples

The following example shows the system executing the power-on of self-tests:

```
sw8-5520(config)# fips self-test poweron
```

Relatedommands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to Flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
show crashinfo console	Reads, writes, and configures crash write to Flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

firewall transparent

To set the firewall mode to transparent mode, use the **firewall transparent** command in global configuration mode. To restore routed mode, use the **no** form of this command. A transparent firewall is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

firewall transparent

no firewall transparent

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system configuration. This command also appears in each context configuration for informational purposes only; you cannot enter this command in a context.

When you change modes, the security appliance clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the security appliance changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command is later in the configuration, the security appliance clears all the preceding lines in the configuration.

Examples

The following example changes the firewall mode to transparent:

```
hostname(config)# firewall transparent
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show firewall	Shows the firewall mode.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

format

To erase all files and format the file system, use the **format** command in privileged EXEC mode. This command erases all files on the file system, including hidden system files, and reinstalls the file system.

format {**disk0: | disk1: | flash:}**

Syntax Description

disk0*:*	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **format** command erases all data on the specified file system and then rewrites the FAT information to the device.

Caution Use the **format** command with extreme caution, only when necessary to clean up corrupted Flash memory.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **format** command.

Note On Cisco PIX security appliances, the **erase** and **format** commands do the same thing, destroy user data with the 0xFF pattern.

To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Note On Cisco ASA 5500 series security appliances, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Examples

This example shows how to format the Flash memory:

```
hostname# format flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the Flash memory.
fsck	Repairs a corrupt file system.

forward interface

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **forward interface** command in interface configuration mode to restore connectivity for one VLAN from initiating contact to one other VLAN. To restrict one VLAN from initiating contact to one other VLAN, use the **no** form of this command. You might need to restrict one VLAN depending on how many VLANs your license supports.

forward interface vlan *number*

no forward interface vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

Defaults

By default, all interfaces can initiate traffic to all other interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In routed mode, you can configure up to three active VLANs with the ASA 5505 adaptive security appliance Base license, and up to five active VLANs with the Security Plus license. An active VLAN is a VLAN with a **nameif** command configured. You can configure up to five inactive VLANs on the ASA 5505 adaptive security appliance for either license, but if you make them active, be sure to follow the guidelines for your license.

With the Base license, the third VLAN must be configured with the **no forward interface** command to restrict this VLAN from initiating contact to one other VLAN.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside work network, and a third VLAN assigned to your home network. The home network does not need to access the work network, so you can use the **no forward interface** command on the home VLAN; the work network can access the home network, but the home network cannot access the work network.

If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance.

Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
backup interface	Assigns an interface to be a backup link to an ISP, for example.
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
switchport access vlan	Assigns a switch port to a VLAN.

fqdn

To include the indicated FQDN in the Subject Alternative Name extension of the certificate during enrollment, use the **fqdn** command in crypto ca trustpoint configuration mode. To restore the default setting of the fqdn, use the **no** form of the command.

fqdn [*fqdn* | **none**]

no fqdn

Syntax Description

fqdn	Specifies the fully qualified domain name. The maximum length of *fqdn* is 64 characters.
none	Specifies no fully qualified domain name.

Defaults

The default setting does not include the FQDN.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If you are configuring the security appliance to support authentication of a Nokia VPN Client using certificates, use the **none** keyword. See the **crypto isakmp identity** or **isakmp identity** command for more information on supporting certificate authentication of the Nokia VPN Client.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the FQDN engineering in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

Command	Description
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

fragment

To provide additional management of packet fragmentation and improve compatibility with NFS, use the **fragment** command in global configuration mode. To return to the default values, use the **no** form of this command.

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

Syntax Description

chain *limit*	Specifies the maximum number of packets into which a full IP packet can be fragmented.
interface	(Optional) Specifies the security appliance interface. If an interface is not specified, the command applies to all interfaces.
size *limit*	Sets the maximum number of packets that can be in the IP reassembly database waiting for reassembly.
timeout *limit*	Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Defaults

The defaults are as follows:

- **chain** is 24 packets
- *interface* is all interfaces
- **size** is 200
- **timeout** is 5 seconds

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified so that you now must choose one of the following arguments: **chain**, **size**, or **timeout**. You can no longer enter the **fragment** command without entering one of these arguments, as was supported in prior releases of the software.

Usage Guidelines

By default, the security appliance accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the security appliance to prevent fragmented packets from traversing the security appliance by entering the **fragment chain 1** *interface* command on each interface. Setting the limit to 1 means that all packets must be whole; that is, unfragmented.

If a large percentage of the network traffic through the security appliance is NFS, additional tuning might be necessary to avoid database overflow.

In an environment where the MTU size is small between the NFS server and client, such as a WAN interface, the **chain** keyword might require additional tuning. In this case, we recommend using NFS over TCP to improve efficiency.

Setting the **size** *limit* to a large value can make the security appliance more vulnerable to a DoS attack by fragment flooding. Do not set the **size** *limit* equal to or greater than the total number of blocks in the 1550 or 16384 pool.

The default values will limit DoS attacks caused by fragment flooding.

Examples

The following example shows how to prevent fragmented packets on the outside and inside interfaces:

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

Continue entering the **fragment chain 1** *interface* command for each additional interface on which you want to prevent fragmented packets.

The following example shows how to configure the fragment database on the outside interface to a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

frequency

To set the rate at which the selected SLA operation repeats, use the **frequency** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description

seconds	The number of seconds between SLA probes. Valid values are from 1 to 604800 seconds. This value cannot be less than the **timeout** value.

Defaults

The default frequency is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An SLA operation repeats at a given frequency for the lifetime of the operation. For example, an **ipIcmpEcho** operation with a frequency of 60 seconds repeats by sending the echo request packets once every 60 seconds for the lifetime of the operation. For example, the default number of packets in an echo operation is 1. This packet is sent when the operation is started and is then sent again 60 seconds later.

If an individual SLA operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is increased rather than immediately repeating the operation.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 3 seconds, and the timeout value us set to 1000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
```

```
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time the SLA operation waits for a response.

fsck

To perform a file system check and to repair corruptions, use the **fsck** command in privileged EXEC mode.

fsck [/no confirm]{**disk0: | disk1: | flash:}**

Syntax Description

/noconfirm	Optional. Do not prompt for confirmation to repair.
disk0*:*	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **fsck** command checks and attempts to repair corrupt file systems. Try using this command before resorting to more permanent procedures.

The **/noconfirm** keyword automatically repairs corruptions without seeking your confirmation first.

Examples

This example shows how to check the file system of the Flash memory:

```
hostname# fsck flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the Flash memory.
format	Erases all files on a file system, including hidden system files, and reinstalls the file system.

ftp mode passive

To set the FTP mode to passive, use the **ftp mode passive** command in global configuration mode. To reset the FTP client to active mode, use the **no** form of this command.

ftp mode passive

no ftp mode passive

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive.The security appliance can use FTP to upload or download image files or configuration files to or from an FTP server. The **ftp mode passive** command controls how the FTP client on the security appliance interacts with the FTP server.

In passive FTP, the client initiates both the control connection and the data connection. Passive mode refers to the server state, in that the server is passively accepting both the control connection and the data connection, which are initiated by the client.

In passive mode, both destination and source ports are ephemeral ports (greater than 1023). The mode is set by the client, as the client issues the **passive** command to initiate the setup of the passive data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

Examples

The following example sets the FTP mode to passive:

```
hostname(config)# ftp mode passive
```

Related Commands

copy	Uploads or downloads image files or configuration files to or from an FTP server.

debug ftp client	Displays detailed information about FTP client activity.
show running-config ftp mode	Displays FTP client configuration.

functions (removed)

You cannot use **functions** command for Release 8.0(2). It is deprecated, and remains in this Command Reference only for reasons of backward compatibility. Use the import and export commands to create URL lists for websites, file access, and plug-ins, customizatioin, and language translations.

To configure automatic downloading of the port forwarding java applet, Citrix support, file access, file browsing, file server entry, application of a webtype ACL, HTTP Proxy, port forwarding, or URL entry over WebVPN for this user or group policy, use the **functions** command in webvpn configuration mode. To remove a configured function, use the **no** form of this command.

functions {**auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | port-forward | none**}

no functions [**auto-download | citrix | file-access | file-browsing | file-entry | filter | url-entry | port-forward**]

Syntax Description

auto-download	Enables or disables automatic download of the port forwarding java applet upon WebVPN login. You must first enable port forwarding, Outlook/Exchange proxy, or HTTP proxy.
citrix	Enables or disables support for terminal services from a MetaFrame Application Server to the remote user. This keyword lets the security appliance act as a secure gateway within a secure Citrix configuration. These services provide users with access to MetaFrame applications through a standard Web browser.
file-access	Enables or disables file access. When enabled, the WebVPN home page lists file servers in the server list. You must enable file access to enable file browsing and/or file entry.
file-browsing	Enables or disables browsing for file servers and shares. You must enable file browsing to allow user entry of a file server.
file-entry	Enables or disables user ability to enter names of file servers.
filter	Applies a webtype ACL. When enabled, the security appliance applies the webtype ACL defined with the webvpn **filter** command.
http-proxy	Enables or disables the forwarding of an HTTP applet proxy to the remote user. The proxy is useful for technologies that interfere with proper mangling, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.
none	Sets a null value for all WebVPN **functions**. Prevents inheriting functions from a default or specified group policy.

port-forward	Enables port forwarding. When enabled, the security appliance uses the port forwarding list defined with the webvpn **port-forward** command.
url-entry	Enables or disables user entry of URLs. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.

Defaults

Functions are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was deprecated.
7.1(1)	The auto-download and citrix keywords were added.
7.0(1)	This command was introduced.

Usage Guidelines

To remove all configured functions, including a null value created by issuing the **functions none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting function values, use the **functions none** command.

Examples

The following example shows how to configure file access and file browsing for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

CHAPTER 13

gateway through hw-module module shutdown Commands

gateway

To specify which group of call agents are managing a particular gateway, use the **gateway** command in MGCP map configuration mode. To remove the configuration, use the **no** form of this command.

gateway *ip_address* [*group_id*]

Syntax Description

gateway	Specifies the group of call agents that are managing a particular gateway
ip_address	The IP address of the gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
MGCP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip_address* option. The *group_id* option is a number from 0 to 4294967295 that must correspond with the *group_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

global

To create a pool of mapped addresses for NAT, use the **global** command in global configuration mode. To remove the pool of addresses, use the **no** form of this command.

global (*mapped_ifc) nat_id* {*mapped_ip*[*-mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[*-mapped_ip*] [**netmask** *mask*] | **interface**}

Syntax Description

interface	Uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP.
mapped_ifc	Specifies the name of the interface connected to the mapped IP address network.
mapped_ip[*-mapped_ip*]	Specifies the mapped address(es) to which you want to translate the real addresses when they exit the mapped interface. If you specify a single address, then you configure PAT. If you specify a range of addresses, then you configure dynamic NAT. If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC).
nat_id	Specifies an integer for the NAT ID. This ID is referenced by the **nat** command to associate a mapped pool with the real addresses to translate. For regular NAT, this integer is between 1 and 2147483647. For policy NAT (**nat id access-list**), this integer is between 1 and 65535. Do not specify a **global** command for NAT ID 0; 0 is reserved for identity NAT and NAT exemption, which do not use a **global** command.
netmask *mask*	(Optional) Specifies the network mask for the *mapped_ip*. This mask does not specify a network when paired with the *mapped_ip*; rather, it specifies the subnet mask assigned to the *mapped_ip* when it is assigned to a host. If you want to configure a range of addresses, you need to specify *mapped_ip-mapped_ip*. If you do not specify a mask, then the default mask for the address class is used.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	NAT is now supported in transparent firewall mode.

Usage Guidelines

For dynamic NAT and PAT, you first configure a **nat** command identifying the real addresses on a given interface that you want to translate. Then you configure a separate **global** command to specify the mapped addresses when exiting another interface (in the case of PAT, this is one address). Each **nat** command matches a **global** command by comparing the NAT ID, a number that you assign to each command.

See the **nat** command for more information about dynamic NAT and PAT.

If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using **clear xlate** command. However, clearing the translation table disconnects all of the current connections.

Examples

For example, to translate the 10.1.1.0/24 network on the inside interface, enter the following command:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

To identify a pool of addresses for dynamic NAT as well as a PAT address for when the NAT pool is exhausted, enter the following commands:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

To translate the lower security dmz network addresses so they appear to be on the same network as the inside network (10.1.1.0), for example, to simplify routing, enter the following commands:

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

To identify a single real address with two different destination addresses using policy NAT, enter the following commands:

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

To identify a single real address/destination address pair that use different ports using policy NAT, enter the following commands:

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

Related Commands

Command	Description
clear configure global	Removes **global** commands from the configuration.
nat	Specifies the real addresses to translate.
show running-config global	Displays the **global** commands in the configuration.
static	Configures a one-to-one translation.

group-alias

To create one or more alternate names by which the user can refer to a tunnel-group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

group-alias *name* [**enable** | **disable]**

no group-alias *name*

Syntax Description

disable	Disables the group alias.
enable	Enables a previously disabled group alias.
name	Specifies the name of a tunnel group alias. This can be any string you choose, except that the string cannot contain spaces.

Defaults

No default group alias, but if you do specify a group alias, that alias is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The group alias that you specify here appears in the drop-down list on the login page. Each group can have multiple aliases or no alias. This command is useful when the same group is known by several common names, such as “Devtest” and “QA”.

Examples

The following example shows the commands for configuring the webvpn tunnel group named “devtest” and establishing the aliases “QA” and “Fra-QA” for the group:

```
hostname(config)# tunnel-group devtest type webvpn
hostname(config)# tunnel-group devtest webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias QA
hostname(config-tunnel-webvpn)# group-alias Fra-QA
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or the named tunnel group configuration.
show webvpn group-alias	Displays the aliases for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the tunnel-group webvpn configuration mode for configuring WebVPN tunnel-group attributes.

group-delimiter

To enable group-name parsing and specify the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **group-delimiter** command in global configuration mode. To disable this group-name parsing, use the **no** form of this command.

group-delimiter *delimiter*

no group-delimiter

Syntax Description

delimiter	Specifies the character to use as the group-name delimiter. Valid values are: **@**, **#**, and **!**.

Defaults

By default, no delimiter is specified, disabling group-name parsing.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The delimiter is used to parse tunnel group names from user names when tunnels are negotiated. By default, no delimiter is specified, disabling group-name parsing.

Examples

This example shows the **group-delimiter** command to change the group delimiter to the hash mark (#):

```
hostname(config)# group-delimiter #
```

Related Commands

Command	Description
clear configure group-delimiter	Clears the configured group delimiter.
show running-config group-delimiter	Displays the current group-delimiter value.
strip-group	Enables or disables strip-group processing.

group-lock

To restrict remote users to access through the tunnel group only, issue the **group-lock** command in group-policy configuration mode or username configuration mode.

To remove the **group-lock** attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy.

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

Syntax Description

none	Sets group-lock to a null value, thereby allowing no group-lock restriction. Prevents inheriting a group-lock value from a default or specified group policy.
value *tunnel-grp-name*	Specifies the name of an existing tunnel group that the security appliance requires for the user to connect.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policyconfiguration	•	—	•	—	—
Username configuration	•	—	•	—	—

Usage Guidelines

To disable group-lock, use the **group-lock none** command.

Group-lock restricts users by checking if the group configured in the VPN Client is the same as the tunnel group to which the user is assigned. If it is not, the security appliance prevents the user from connecting. If you do not configure group-lock, the security appliance authenticates users without regard to the assigned group.

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set group lock for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

To add network object groups, use the **group-object** command in protocol, network, service, and icmp-type configuration modes. To remove network object groups, use the **no** form of this command.

group-object *obj_grp_id*

no group-object *obj_grp_id*

Syntax Description

obj_grp_id	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Protocol, network, service, icmp-type configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **group-object** command is used with the **object-group** command to define an object that itself is an object group. It is used in protocol, network, service, and icmp-type configuration modes. This sub-command allows logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

Duplicate objects are allowed in an object group if they are group objects. For example, if object 1 is in both group A and group B, it is allowed to define a group C which includes both A and B. It is not allowed, however, to include a group object which causes the group hierarchy to become circular. For example, it is not allowed to have group A include group B and then also have group B include group A.

The maximum allowed levels of a hierarchical object group is 10.

Examples

The following example shows how to use the **group-object** command in network configuration mode eliminate the need to duplicate hosts:

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
```

```
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

Syntax Description

external server-group *server_group*	Specifies the group policy as external and identifies the AAA server group for the security appliance to query for attributes.
from *group-policy_name*	Initializes the attributes of this internal group policy to the values of a pre-existing group policy.
internal	Identifies the group policy as internal.
name	Specifies the name of the group policy. The name can be up to 64 characters long and cannot contain spaces.
password *server_password*	Provides the password to use when retrieving attributes from the external AAA server group. The password can be up to 128 characters long and cannot contain spaces.

Defaults

No default behavior or values. See Usage Guidelines.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

A default group policy, named "DefaultGroupPolicy," always exists on the security appliance. However, this default group policy does not take effect unless you configure the security appliance to use it. For configuration instructions, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Use the **group-policy attributes** command to enter config-group-policy mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

In addition, you can configure webvpn-mode attributes for the group policy, either by entering the **webvpn** command in config-group-policy mode or by entering the **group-policy attributes** command and then entering the **webvpn** command in config-group-webvpn mode. See the description of the **group-policy attributes** command for details.

Examples

The following example shows how to create an internal group policy with the name “FirstGroup”:

```
hostname(config)# group-policy FirstGroup internal
```

The next example shows how to create an external group policy with the name “ExternalGroup,” the AAA server group “BostonAAA,” and the password “12345678”:

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn mode to configure webvpn attributes for the group.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

group-policy attributes

To enter the config-group-policy mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, user the **no** version of this command. In config-group-policy mode, you can configure Attribute-Value Pairs for a specified group policy or enter group-policy webvpn configuration mode to configure webvpn attributes for the group.

group-policy *name* **attributes**

no group-policy *name* **attributes**

Syntax Description

name	Specifies the name of the group policy.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

The syntax of the commands in attributes mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration, and enables inheritance of a value from another group policy.
- The **none** keyword sets the attribute in the running configuration to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

A default group policy, named DefaultGroupPolicy, always exists on the security appliance. However, this default group policy does not take effect unless you configure the security appliance to use it. For configuration instructions, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

The **group-policy attributes** command enters config-group-policy mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
backup-servers	keep-client-config
banner	none

Attribute	Default Value
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

In addition, you can configure webvpn-mode attributes for the group policy, by entering the **group-policy attributes** command and then entering the **webvpn** command in config-group-policy mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter group-policy attributes mode for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy	Creates, edits, or removes a group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn (group-policy attributes mode)	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

group-prompt

To customize the group prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **group-prompt** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

group-prompt {**text** | **style**} *value*

no group-prompt {**text** | **style**} *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text of the group prompt is “GROUP:”.

The default style of the group prompt is color:black;font-weight:bold;text-align:right.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Group:", and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# group-prompt text Corporate Group:
F1-asa1(config-webvpn-custom)# group-prompt style font-weight:bolder
```

Related Commands

Command	Description
password-prompt	Customizes the password prompt of the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page.

group-search-timeout

To specify the maximum time to wait for a response from an Active Directory server queried using the **show ad-groups** command, use the **group-search-timeout** command in AAA server host configuration mode. To remove the command from the configuration, use the **no** form of the command:

group-search-timeout *seconds*

no group-search-timeout *seconds*

Syntax Description

seconds	The time to wait for a response from the Active Directory server, from 1 to 300 seconds.

Defaults

The default is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command is introduced.

Usage Guidelines

The **show ad-groups** command applies only to Active Directory servers using LDAP, and displays groups that are listed on an Active Directory server. Use the **group-search-timeout** command to adjust the time to wait for a response from the server.

Examples

The following example sets the timeout to 20 seconds:

```
hostname(config-aaa-server-host)#group-search-timeout 20
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
show ad-groups	Displays groups that are listed on an Active Directory server.

group-url

To specify incoming URLs or IP addresses for the group, use the **group-url** command in tunnel-group webvpn configuration mode. To remove a URL from the list, use the **no** form of this command.

group-url *url* [**enable** | **disable**]

no group-url *url*

Syntax Description

disable	Disables the URL, but does not remove it from the list.
enable	Enables the URL.
url	Specifies a URL or IP address for this tunnel group.

Defaults

There is no default URL or IP address, but if you do specify a URL or IP address, it is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Specifying a group URL or IP address eliminates the need for the user to select a group at login. When a user logs in, the security appliance looks for the user's incoming URL/address in the tunnel-group-policy table. If it finds the URL/address and if group-url is enabled in the tunnel group, then the security appliance automatically selects the associated tunnel group and presents the user with only the username and password fields in the login window. This simplifies the user interface and has the added advantage of never exposing the list of groups to the user. The login window that the user sees uses the customizations configured for that tunnel group.

If the URL/address is disabled and group-alias is configured, then the dropdown list of groups is also displayed, and the user must make a selection.

You can configure multiple URLs/addresses (or none) for a group. Each URL/address can be enabled or disabled individually. You must use a separate **group-url** command for each URL/address specified. You must specify the entire URL/address, including either the http or https protocol.

You cannot associate the same URL/address with multiple groups. The security appliance verifies the uniqueness of the URL/address before accepting the URL/address for a tunnel group.

The following example shows the commands for configuring the webvpn tunnel group named “test” and establishing two group URLs, “http://www.cisco.com” and “https://supplier.com” for the group:

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com
hostname(config-tunnel-webvpn)# group-url https://supplier.company.com
hostname(config-tunnel-webvpn)#
```

The following example enables the group URLs http://www.cisco.com and http://192.168.10.10 for the tunnel-group named RadiusServer:

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias “Cisco Remote Access” enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or the named tunnel group configuration.
show webvpn group-url	Displays the URLs for the specified tunnel group or for all tunnel groups.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

h245-tunnel-block

To block H.245 tunneling in H.323, use the **h245-tunnel-block** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

h245-tunnel-block action [drop-connection | log]

no h245-tunnel-block action [drop-connection | log]

Syntax Description

drop-connection	Drops the call setup connection when H.245 tunnel is detected.
log	Issues a log when H.245 tunnel is detected.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to block H.245 tunneling on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# h245-tunnel-block action drop-connection
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

hello-interval

To specify the interval between EIGRP hello packets sent on an interface, use the **hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.
seconds	Specifies the interval between hello packets that are sent on the interface; valid values are from 1 to 65535 seconds.

Defaults

The default *seconds* is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hold-time	Configures the EIGRP hold time advertised in hello packets.

help

To display help information for the command specified, use the **help** command in user EXEC mode.

help {*command* | **?**}

Syntax Description

command	Specifies the command for which to display the CLI help.
?	Displays all commands that are available in the current privilege level and mode.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **help** command displays help information about all commands. You can see help for an individual command by entering the **help** command followed by the command name. If you do not specify a command name and enter **?** instead, all commands that are available in the current privilege level and mode display.

If you enable the **pager** command and when 24 lines display, the listing pauses, and the following prompt appears:

```
<--- More --->
```

The More prompt uses syntax similar to the UNIX **more** command as follows:

- To see another screen of text, press the **Space** bar.
- To see the next line, press the **Enter** key.
- To return to the command line, press the **q** key.

Examples

The following example shows how to display help for the **rename** command:

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
```

```
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

The following examples shows how to display help by entering the command name and a question mark:

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

Help is available for the core commands (not the **show**, **no**, or **clear** commands) by entering **?** at the command prompt:

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

hic-fail-group-policy (deprecated)

To specify a group policy to grant a WebVPN user access rights that are different from the default group policy, use the **hic-fail-group-policy** command in tunnel-group-webvpn configuration mode. The **no** form of this command sets the group policy to the default group policy.

hic-fail-group-policy *name*

no hic-fail-group-policy

Syntax Description

name	Specifies the name of the group policy.

Defaults

DfltGrpPolicy

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group-webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(2)	This command was deprecated.

Usage Guidelines

This command is valid only for security appliances with Cisco Secure Desktop installed. Host integrity checking, also called *System Detection*, involves checking the remote PC for a minimal set of criteria that must be satisfied to apply a VPN feature policy. The security appliance uses the value of the hic-fail-group-policy attribute to limit access rights to remote CSD users as follows:

- Always uses it if you set the VPN feature policy to “Use Failure Group-Policy.”
- Uses it if you set the VPN feature policy to “Use Success Group-Policy, if criteria match” and the criteria then fail to match.

This attribute specifies the name of the failure group policy to be applied. Use a group policy to differentiate access rights from those associated with the default group policy.

Note The security appliance does not use this attribute if you set the VPN feature policy to “Always use Success Group-Policy.”

For more information, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*.

Examples

The following example creates a WebVPN tunnel group named “FirstGroup” and specifies the failure group policy with the name “group2”:

```
hostname(config)# tunnel-group FirstGroup webvpn
hostname(config)# tunnel-group FirstGroup webvpn-attributes
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
tunnel-group webvpn-attributes	Specifies the WebVPN attributes for the named tunnel-group.

hidden-parameter

To specify hidden parameters in the HTTP POST request that the security appliance submits to the authenticating web server for SSO authentication, use the **hidden-parameter** command in aaa-server-host configuration mode. To remove all hidden parameters from the running configuration, use the **no** form of this command.

hidden-parameter *string*

no hidden-parameter

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	A hidden parameter embedded in the form and sent to the SSO server. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for all lines together—the complete hidden parameter—is 2048.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

This is an SSO with HTTP Forms command.

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. That request may require specific hidden parameters from the SSO HTML form—other then username and password—that are not visible to the user. You can discover hidden parameters that the web server expects in the POST request by using a HTTP header analyzer on a form received from the web server.

The command **hidden-parameter** lets you specify a hidden parameter the web server requires in the authentication POST request. If you use a header analyzer, you can copy and paste the whole hidden parameter string including any encoded URL parameters.

For ease of entry, you can enter a hidden parameter on multiple, sequential lines. The security appliance then concatenates the lines into a single hidden parameter. While the maximum characters per hidden-parameter line is 255 characters, you can enter fewer characters on each line.

Note Any question mark in the string must be preceded by a CTRL-v escape sequence.

Examples

The following example shows a hidden parameter comprised of four form entries and their values, separated by &. Excerpted from the POST request, the four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do %3FEMCOPageCode%3DENG
- smauthreason with a value of 0

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter t=https%3A%2F%2Ftools.cisco.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

hidden-shares

To control the visibility of hidden shares for CIFS files, use the **hidden-shares** command in config-group-webvpn configuration mode. To remove the hidden shares option from the configuration, use the **no** form of this command.

hidden-shares {none | visible}

[no] hidden-shares {none | visible}

Syntax Description

none	Specifies that no configured hidden shares are visible or accessible to users.
visible	Reveals hidden shares, making them accessible to users.

Defaults

The default behavior for this command is none.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Group-webvpn configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A hidden share is identified by a dollar sign ($) at the end of the share name. For example, drive C is shared as C$. With hidden shares, a shared folder is not displayed, and users are restricted from browsing or accessing these hidden resources.

The **no** form of the **hidden-shares** command removes the option from the configuration and disables hidden shares as a group policy attribute.

Examples

The following example makes visible WebVPN CIFS hidden-shares related to GroupPolicy2:

```
hostname(config)# webvpn
hostname(config-group-policy)#  group-policy GroupPolicy2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# hidden-shares visible
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
debug webvpn cifs	Displays debug messages about the CIFS.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter WebVPN mode to configure WebVPN attributes for the group.
url-list	(Global Configuration Mode) Configures a set of URLs for WebVPN users to access.
url-list	(WebVPN Mode) Applies a list of WebVPN servers and URLs to a particular user or group policy.

hold-time

To specify the hold time advertised by the security appliance in EIGRP hello packets, use the **hold-time** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.
seconds	Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds.

Defaults

`The default *seconds* is 15 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the security appliance. The EIGRP neighbors on that interface use this value to determine the availability of the security appliance. If they do not receive a hello packet from the security appliance during the advertised hold time, the EIGRP neighbors will consider the security appliance to be unavailable.

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If the security appliance does not receive a hello packet within the specified hold time, routes through this neighbor are considered unavailable.

Increasing the hold time delays route convergence across the network.

Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

```
hostname(config-if)# hello-interval eigrp 100 10
```

```
hostname(config-if)# hold-time eigrp 100 30
```

Related Commands

Command	Description
hello-interval	Specifies the interval between EIGRP hello packets sent on an interface.

homepage

To specify a URL for the web page that displays upon login for this WebVPN user or group policy, use the **homepage** command in webvpn mode, which you enter from group-policy or username mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, use the **homepage none** command.

homepage {value *url-string* **| none}**

no homepage

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting an home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

Defaults

There is no default home page.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To specify a homepage URL for users associated with the group policy, enter a value for the url-string in this command. To inherit a home page from the default group policy, use the **no** form of the comand. Clientless users are immediately brought to this page after successful authentication. AnyConnect launches the default web browser to this URL upon successful establishment of the VPN connection. On Linux platforms, AnyConnect does not currently support this command and ignores it.

Examples

The following example shows how to specify www.example.com as the home page for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.

host

To specify a host to interact with using RADIUS accounting, use the **host** command in radius-accounting parameter configuration mode, which is accessed by using the **parameters** command in the policy-map type inspect radius-accounting submode. To disable specified host, use the **no** form of this command. This option is disabled by default.

host *address* [**key** *secret*]

no host *address* [**key** *secret*]

Syntax Description

host	Specifies a single endpoint sending the RADIUS accounting messages.
address	The IP address of the client or server sending the RADIUS accounting messages.
key	Optional keyword to specify the secret of the endpoint sending the gratuitous copy of the accounting messages.
secret	The shared secret key of the endpoint sending the accounting messages used to validate the messages. This can be up to 128 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Multiple instances of this command are allowed.

Examples

The following example shows how to specify a host with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# host 209.165.202.128 key cisco123
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

hostname

To set the security appliance hostname, use the **hostname** command in global configuration mode. To restore the default hostname, use the **no** form of this command. The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

hostname *name*

no hostname [*name*]

Syntax Description

name	Specifies a hostname up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

Defaults

The default hostname depends on your platform.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	You can no longer use non-alphanumeric characters (other than a hyphen).

Usage Guidelines

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts.

The hostname that you optionally set within a context does not appear in the command line, but can be used for the **banner** command **$(hostname)** token.

Examples

The following example sets the hostname to firewall1:

```
hostname(config)# hostname firewall1
firewall1(config)#
```

Related Commands

Command	Description
banner	Sets a login, message of the day, or enable banner.
domain-name	Sets the default domain name.

hsi

To add an HSI to an HSI group for H.323 protocol inspection, use the **hsi** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

hsi *ip_address*

no hsi *ip_address*

Syntax Description

ip_address	IP address of the host to add. A maximum of five HSIs per HSI group is allowed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HSI group configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to add an HSI to an HSI group in an H.323 inspection policy map:

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
endpoint	Adds an endpoint to the HSI group.
hsi-group	Creates an HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

hsi-group

To define an HSI group for H.323 protocol inspection and to enter hsi group configuration mode, use the **hsi-group** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

hsi-group *group_id*

no hsi-group *group_id*

Syntax Description

group_id	HSI group ID number (0 to 2147483647).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure an HSI group in an H.323 inspection policy map:

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
endpoint	Adds an endpoint to the HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

html-content-filter

To filter Java, ActiveX, images, scripts, and cookies for WebVPN sessions for this user or group policy, use the **html-content-filter** command in webvpn configuration mode. To remove a content filter, use the **no** form of this command.

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

Syntax Description

cookies	Removes cookies from images, providing limited ad filtering and privacy.
images	Removes references to images (removes <IMG> tags).
java	Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags.
none	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
scripts	Removes references to scripting (removes <SCRIPT> tags).

Defaults

No filtering occurs.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To remove all content filters, including a null value created by issuing the **html-content-filter none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an html content filter, use the **html-content-filter none** command.

Using the command a second time overrides the previous setting.

Examples

The following example shows how to set filtering of JAVA and ActiveX, cookies, and images for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
```

```
hostname(config-group-webvpn)# html-content-filter java cookies images
```

Related Commands

Command	Description
webvpn (group-policy, username)	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

http

To specify hosts that can access the HTTP server internal to the security appliance, use the **http** command in global configuration mode. To remove one or more hosts, use the **no** form of this command. To remove the attribute from the configuration, use the **no** form of this command without arguments.

http *ip_address subnet_mask interface_name*

no http

Syntax Description

interface_name	Provides the name of the security appliance interface through which the host can access the HTTP server.
ip_address	Provides the IP address of a host that can access the HTTP server.
subnet_mask	Provides the subnet mask of a host that can access the HTTP server.

Defaults

No hosts can access the HTTP server.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to allow the host with the IP address of 10.10.99.1 and the subnet mask of 255.255.255.255 access to the HTTP server via the outside interface:

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

The next example shows how to allow any host access to the HTTP server via the outside interface:

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.

Command	Description
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http-comp

To enable compression of http data over a WebVPN connection for a specific group or user, use the **http-comp** command in the group-policy webvpn and username webvpn configuration modes. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

Syntax Description

gzip	Specifies compression is enabled for the group or user.
none	Specifies compression is disabled for the group or user.

Defaults

By default, compression is set to *gzip*.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration	•	—	•	—	—
Username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

For WebVPN connections, the **compression** command configured from global configuration mode overrides the **http-comp** command configured in group policy and username webvpn configuration modes.

Examples

In the following example, compression is disabled for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, IPSec VPN connections.

http-proxy

To configure the security appliance to use an external proxy server to handle HTTP requests, use the **http-proxy** command in webvpn configuration mode. To remove the HTTP proxy server from the configuration, use the **no** form of this command.

http-proxy {*host* [*port*] [**exclude** `url`] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

Syntax Description

host	Hostname or IP address for the external HTTP proxy server.
pac *pacfile*	Identifies the PAC file that contains a JavaScript function that specifies one or more proxies.
password	(Optional, and available only if you specify a *username*) Enter this keyword to accompany each HTTP proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTP request.
port	(Optional) Port number used by the HTTP proxy server. The default port is 80, which is the port the security appliance uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTP proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTP request.

Defaults

By default, no HTTP proxy server is configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	Added **exclude**, **username**, and **password** keywords.
7.0(1)	This command was introduced.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The security appliance supports only one instance of the http-proxy command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any http-proxy commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **http -proxy** command, then none is present.

Examples

The following example shows how to configure use of an HTTP proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 209.165.201.2
hostname(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTP request:

```
hostname(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

The following example shows the same command, except when the security appliance receives the specific URL www.example.com in an HTTP request, it resolves the request instead of passing it on to the proxy server:

```
hostname(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)
```

The followiing example shows how to use the exclude option:

```
hostname(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
hostname(config-webvpn)
```

The followiing example shows how to use the pac option:

```
hostname(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

Related Commands

Command	Description
https-proxy	Configures the use of an external proxy server to handle HTTPS requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

http-proxy (dap)

To enable or disable HTTP proxy port forwarding, use the **http-proxy** command in dap webvpn configuration mode.To remove the attribute from the configuration, use the **no** version of this command.

http-proxy {enable | disable | auto-start}

no http-proxy

Syntax Description

auto-start	Enables and automatically starts HTTP proxy port forwarding for the DAP record.
enable/disable	Enables or disables HTTP proxy port forwarding for the DAP record.

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dap-webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the security appliance applies that value and enforces it. For example, when you disable HTTP proxy in dap webvpn mode, the security appliance looks no further for a value. When you instead use the **no** value for the **http-proxy** command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable HTTP proxy port forwarding for the dynamic access policy record named Finance.

```
hostname (config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# http-proxy enable
hostname(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

http redirect

To specify that the security appliance redirect HTTP connections to HTTPS, use the **http redirect** command in global configuration mode. To remove a specified http redirect command from the configuration, use the **no** version of this command. To remove all http redirect commands from the configuration, use the **no** version of this command without arguments.

http redirect *interface* [*port*]

no http redirect [*interface*]

Syntax Description

interface	Identifies the interface for which the security appliance should redirect HTTP requests to HTTPS.
port	Identifies the port the security appliance listens on for HTTP requests, which it then redirects to HTTPS. By default it listens on port 80,

Defaults

HTTP redirect is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The interface requires an access list that permits HTTP. Otherwise the security appliance does not listen to port 80, or to any other port that you configure for HTTP.

Examples

The following example shows how to configure HTTP redirect for the inside interface, keeping the default port 80:

```
hostname(config)# http redirect inside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server enable

To enable the security appliance HTTP server, use the **http server enable** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

http server enable [*port*]

Syntax Description

port	The port to use for HTTP connections. The range is 1-65535. The default port is 443.

Defaults

The HTTP server is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to enable the HTTP server.

```
hostname(config)# http server enable
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

https-proxy

To configure the security appliance to use an external proxy server to handle HTTPS requests, use the **https-proxy** command in webvpn configuration mode. To remove the HTTPS proxy server from the configuration, use the **no** form of this command.

https-proxy {*host* [*port*] [**exclude** `url`] | [**username** *username* {**password** *password*}]

no https-proxy

Syntax Description

host	Hostname or IP address for the external HTTPS proxy server.
password	(Optional, and available only if you specify a *username*) Enter this keyword to accompany each HTTPS proxy request with a password to provide basic, proxy authentication.
password	Password to send to the proxy server with each HTTPS request.
port	(Optional) Port number used by the HTTPS proxy server. The default port is 443, which is the port the security appliance uses if you do not supply a value. The range is 1-65535.
url	Enter a URL or a comma-delimited list of several URLs to exclude from those that can be sent to the proxy server. The string does not have a character limit, but the entire command cannot exceed 512 characters. You can specify literal URLs or use the following wildcards: • ***** to match any string, including slashes (/) and periods (.). You must accompany this wildcard with an alphanumeric string. • **?** to match any single character, including slashes and periods. • [*x*-*y*] to match any single character in the range of *x* and *y*, where *x* represents one character and *y* represents another character in the ANSI character set. • [**!***x*-*y*] to match any single character that is not in the range.
username	(Optional) Enter this keyword to accompany each HTTPS proxy request with a username to provide basic, proxy authentication.
username	Username to send to the proxy server with each HTTPS request.

Defaults

By default, no HTTPS proxy server is configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	Added **exclude**, **username**, and **password** keywords.
7.0(1)	This command was introduced.

Usage Guidelines

Requiring Internet access via a server that the organization controls provides another opportunity for filtering to assure secure Internet access and administrative control.

The security appliance supports only one instance of the https-proxy command. If one instance of this command is already present in the running configuration and you enter another instance, the CLI overwrites the previous instance. The CLI lists any https-proxy commands in the running configuration if you enter the **show running-config webvpn** command. If the response does not list an **https-proxy** command, then none is present.

Examples

The following example shows how to configure use of an HTTPS proxy server with an IP address of 209.165. 201.2 using the default port, 443:

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 209.165.201.2
hostname(config-webvpn)
```

The following example shows how to configure use of the same proxy server, and send a username and password with each HTTPS request:

```
hostname(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

The following example shows the same command, except when the security appliance receives the specific URL www.example.com in an HTTPS request, it resolves the request instead of passing it on to the proxy server:

```
hostname(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)

hostname(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
hostname(config-webvpn)
```

The followiing example shows how to use the pac option:

```
hostname(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

Related Commands

Command	Description
http-proxy	Configures the use of an external proxy server to handle HTTP requests.
show running-config webvpn	Displays the running configuration for SSL VPN, including any HTTP and HTTPS proxy servers.

hw-module module password-reset

To reset the password on the hardware module to the default value, "cisco," use the **hw-module module password reset** command in privileged EXEC mode.

hw-module module slot# password-reset

Syntax Description

slot#	Specifies the slot number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

This command is only valid when the hardware module is in the Up state and supports password reset. On the AIP SSM, running this command results in rebooting of the module. The module is offline until the rebooting is finished, which may take several minutes. You can run the **show module** command to monitor the module state.

The command always prompts for confirmation. If the command succeeds, no other output appears. If the command fails, an error message appears that explains why the failure occurred. The possible error messages are as follows:

```
Unable to reset the password on the module in slot 1

Unable to reset the password on the module in slot 1 - unknown module state

Unable to reset the password on the module in slot 1 - no module installed

Failed to reset the password on the module in slot 1 - module not in Up state

Unable to reset the password on the module in slot 1 - unknown module type

The module is slot [n] does not support password reset

Unable to reset the password on the module in slot 1 - no application found

The SSM application version does not support password reset

Failed to reset the password on the module in slot 1
```

Examples

The following example resets a password on a hardware module in slot 1:

```
hostname (config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

Related Commands

Command	Description
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module reset	Shuts down and resets the SSM hardware.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module recover

To load a recovery software image from a TFTP server to an intelligent SSM (for example, the AIP SSM), or to configure network settings to access the TFTP server, use the **hw-module module recover** command in privileged EXEC mode. You might need to recover an SSM using this command if, for example, the SSM is unable to load a local image. This command is not available for interface SSMs (for example, the 4GE SSM).

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *port_ip_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

Syntax Description

1	Specifies the slot number, which is always 1.
boot	Initiates recovery of this SSM and downloads a recovery image according to the **configure** settings. The SSM then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter any network parameters after the **configure** keyword, you are prompted for the information.
gateway *gateway_ip_address*	(Optional) The gateway IP address for access to the TFTP server through the SSM management interface.
ip *port_ip_address*	(Optional) The IP address of the SSM management interface.
stop	Stops the recovery action, and stops downloading the recovery image. The SSM boots from the original image. You must enter this command within 30 to 45 seconds after starting recovery using the **hw-module module boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the SSM becoming unresponsive.
url *tfp_url*	(Optional) The URL for the image on a TFTP server, in the following format: **tftp:**//*server*/[*path*/]*filename*
vlan *vlan_id*	(Optional) Sets the VLAN ID for the management interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is only available when the SSM is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information.

Examples

The following example sets the SSM to download an image from a TFTP server:

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

The following example recovers the SSM:

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module reload

To reload an intelligent SSM software (for example, the AIP SSM), use the **hw-module module reload** command in privileged EXEC mode. This command is not available for interface SSMs (for example, the 4GE SSM).

hw-module module 1 reload

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is only valid when the SSM status is Up. See the **show module** command for state information.

This command differs from the **hw-module module reset** command, which also performs a hardware reset.

Examples

The following example reloads the SSM in slot 1:

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

Command	Description
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module reset

To shut down and reset the SSM hardware, use the **hw-module module reset** command in privileged EXEC mode.

hw-module module 1 reset

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is only valid when the SSM status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

When the SSM is in an Up state, the **hw-module module reset** command prompts you to shut down the software before resetting.

You can recover intelligent SSMs (for example, the AIP SSM) using the **hw-module module recover** command. If you enter the **hw-module module reset** while the SSM is in a Recover state, the SSM does not interrupt the recovery process. The **hw-module module reset** command performs a hardware reset of the SSM, and the SSM recovery continues after the hardware reset. You might want to reset the SSM during recovery if the SSM hangs; a hardware reset might resolve the issue.

This command differs from the **hw-module module reload** command, which only reloads the software and does not perform a hardware reset.

Examples

The following example resets an SSM in slot 1 that is in the Up state:

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

```
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module shutdown

To shut down the SSM software, use the **hw-module module shutdown** command in privileged EXEC mode.

hw-module module 1 shutdown

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Shutting down the SSM software prepares the SSM to be safely powered off without losing configuration data.

This command is only valid when the SSM status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down an SSM in slot 1:

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

Command	Description
hw-module module reload	Reloads the intelligent SSM software.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
show module	Shows SSM information.

CHAPTER 14

icmp through import webvpn webcontent Commands

icmp

To configure access rules for ICMP traffic that terminates at a security appliance interface, use the **icmp** command. To remove the configuration, use the **no** form of this command.

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

deny	Deny access if the conditions are matched.
icmp_type	(Optional) ICMP message type (see Table 3).
if_name	The interface name.
ip_address	The IP address of the host sending ICMP messages to the interface.
net_mask	The mask to be applied to *ip_address*.
permit	Permit access if the conditions are matched.

Defaults

The default behavior of the security appliance is to allow all ICMP traffic *to* the security appliance interfaces. However, by default the security appliance does not respond to ICMP echo requests directed to a broadcast address. The security appliance also denies ICMP messages received at the outside interface for destinations on a protected interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
6.0	This command was introduced.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any security appliance interface. If no ICMP control list is configured, then the security appliance accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address.

The **icmp deny** command disables pinging to an interface, and the **icmp permit** command enables pinging to an interface. With pinging disabled, the security appliance cannot be detected on the network. This is also referred to as configurable proxy pinging.

Use the **access-list extended** or **access-group** commands for ICMP traffic that is routed *through* the security appliance for destinations on a protected interface.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPSec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If an ICMP control list is configured for an interface, then the security appliance first matches the specified ICMP traffic and then applies an implicit deny for all other ICMP traffic on that interface. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a **permit** statement is assumed.

Table 3 lists the supported ICMP type values.

Table 14-1 ICMP Types and Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
8	echo
11	time-exceeded

Examples

The following example denies all ping requests and permits all unreachable messages at the outside interface:

```
hostname(config)# icmp permit any unreachable outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

The following example permits host 172.16.2.15 or hosts on subnet 172.22.1.0/16 to ping the outside interface:

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

icmp unreachable

To configure the unreachable ICMP message rate limit for ICMP traffic that terminates at a security appliance interface, use the **icmp unreachable** command. To remove the configuration, use the **no** form of this command.

icmp unreachable rate-limit *rate* **burst-size** *size*

no icmp unreachable rate-limit *rate* **burst-size** *size*

Syntax Description

rate-limit *rate*	Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
burst-size *size*	Sets the burst rate, between 1 and 10. This keyword is not currently used by the system, so you can choose any value.

Defaults

The default rate limit is 1 message per second.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

If you allow ICMP messages, including unreachable messages, to terminate on a security appliance interface (see the **icmp** command), then you can control the rate of unreachable messages.

This command, along with the **set connection decrement-ttl** command, is required to allow a traceroute through the security appliance that shows the security appliance as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
set connection decrement-ttl	Decrements the time to live value for a packet.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

icmp-object

To add icmp-type object groups, use the **icmp-object** command in icmp-type configuration mode. To remove network object groups, use the **no** form of this command.

icmp-object *icmp_type*

no group-object *icmp_type*

Syntax Description

icmp_type	Specifies an icmp-type name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Icmp-type configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **icmp-object** command is used with the **object-group** command to define an icmp-type object. It is used in icmp-type configuration mode.

ICMP type numbers and names include:

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**

Number	ICMP Type Name
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

Examples

The following example shows how to use the **icmp-object** command in icmp-type configuration mode:

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

id-cert-issuer

To indicate whether the system accepts peer certificates issued by the CA associated with this trustpoint, use the **id-cert-issuer** command in crypto ca-trustpoint configuration mode. Use the **no** form of this command to disallow certificates that were issued by the CA associated with the trustpoint. This is useful for trustpoints that represent widely used root CAs.

id-cert-issuer

no id-cert-issuer

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is enabled (identity certificates are accepted).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca-trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use this command to limit certificate acceptance to those issued by the subordinate certificate of a widely used root certificate. If you do not allow this feature, the security appliance rejects any IKE peer certificate signed by this issuer.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and lets an administrator accept identity certificates signed by the issuer for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint submode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

id-mismatch

To enable logging for excessive DNS ID mismatches, use the **id-mismatch** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] [**action log**]

Syntax Description

count *number*	The maximum number of mismatch instances before a system message log is sent.
duration *seconds*	The period, in seconds, to monitor.

Defaults

This command is disabled by default. The default rate is 30 in the a period of 3 seconds if the options are not specified when the command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

A high rate of DNS ID mismatches may indicate a cache poisoning attack. This command can be enabled to monitor and alert such attempts. A summarized system message log will be printed if the mismatch rate exceeds the configured value. The **id-mismatch** command provides the system administrator with additional information to the regular event-based system message log.

Examples

The following example shows how to enable ID mismatch in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-mismatch action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-randomization

To randomize the DNS identifier for a DNS query, use the **id-randomization** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

id-randomization

no id-randomization

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled by default. The DNS identifier from the DNS query does not get modified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

ID randomization helps protect against cache poisening attacks.

Examples

The following example shows how to enable ID randomization in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-randomization
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

id-usage (crypto ca trustpoint)

To specify how the enrolled identity of a certificate can be used, use the **id-usage** command in crypto ca trustpoint configuration mode. To set the usage of the certificate to the default, **ssl-ipsec**, use the **no** form of this command.

id-usage {ssl-ipsec | code-signer}

no id-usage {ssl-ipsec | code-signer}

Syntax Description

code-signer	The device identity represented by this certificate is used as a Java code signer to verify applets provided to remote users.
ssl-ipsec	(Default) The device identity represented by this certificate can be used as the server-side identity for SSL or IPSec-encrypted connections.

Defaults

The **id-usage** command default is **ssl-ipsec**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Remote-access VPNs can use SSL, IPSec, or both protocols, depending on deployment requirements, to permit access to virtually any network application or resource. The **id-usage** command allows you to specify the type of access to various certificate-protected resources.

A CA identity and in some cases, a device identity, is based on a certificate issued by the CA. All of the commands within the crypto ca trustpoint mode control CA-specific configuration parameters, which specify how the security appliance obtains the CA certificate, how the security appliance obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Only a single instance of the **id-usage** command can be present in a trustpoint configuration. To enable the trustpoint for code-signer and/or ssl-ipsec, use a single instance which can specify either or both options.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and designates it a code-signer certificate:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# id-usage code-signer
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint general, and designates it as both a code-signer certificate and as a server side identity for SSL or IPSec connections:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint checkin1,and resets it to limit its use to SSL or IPSec connections:

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# no id-usage ssl-ipsec
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
java-trustpoint	Configures the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location.
ssl trust-point	Specifies the certificate that represents the SSL certificate for an interface.
trust-point (tunnel-group ipsec-attributes mode)	Specifies the name that identifies the certificate to be sent to the IKE peer,
validation-policy	Specifies conditions for validating certificates associated with user connections.

igmp

To reinstate IGMP processing on an interface, use the **igmp** command in interface configuration mode. To disable IGMP processing on an interface, use the **no** form of this command.

igmp

no igmp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
hostname(config-if)# no igmp
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **igmp access-group** command in interface configuration mode. To disable groups on the interface, use the **no** form of this command.

igmp access-group *acl*

no igmp access-group *acl*

Syntax Description

acl	Name of an IP access list. You can specify a standard or and extended access list. However, if you specify an extended access list, only the destination address is matched; you should specify **any** for the source.

Defaults

All groups are allowed to join on an interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp forward interface

To enable forwarding of all IGMP host reports and leave messages received to the interface specified, use the **igmp forward interface** command in interface configuration mode. To remove the forwarding, use the **no** form of this command.

igmp forward interface *if-name*

no igmp forward interface *if-name*

Syntax Description

if-name	Logical name of the interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Enter this command on the input interface. This command is used for stub multicast routing and cannot be configured concurrently with PIM.

Examples

The following example forwards IGMP host reports from the current interface to the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp join-group

To configure an interface to be a locally connected member of the specified group, use the **igmp join-group** command in interface configuration mode. To cancel membership in the group, use the **no** form of this command.

igmp join-group *group-address*

no igmp join-group *group-address*

Syntax Description

group-address	IP address of the multicast group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command configures a security appliance interface to be a member of a multicast group. The **igmp join-group** command causes the security appliance to both accept and forward multicast packets destined for the specified multicast group.

To configure the security appliance to forward the multicast traffic without being a member of the multicast group, use the **igmp static-group** command.

Examples

The following example configures the selected interface to join the IGMP group 255.2.2.2:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

Related Commands

Command	Description
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp limit

To limit the number of IGMP states on a per-interface basis, use the **igmp limit** command in interface configuration mode. To restore the default limit, use the **no** form of this command.

igmp limit *number*

no igmp limit [*number*]

Syntax Description

number	Number of IGMP states allowed on the interface. Valid values range from 0 to 500. The default value is 500. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the **igmp join-group** and **igmp static-group** commands) are still permitted.

Defaults

The default is 500.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced. It replaced the **igmp max-groups** command.

Examples

The following example limits the number of IGMP states on the interface to 250:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

Related Commands

Command	Description
igmp	Reinstates IGMP processing on an interface.
igmp join-group	Configure an interface to be a locally connected member of the specified group.
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

To configure the frequency at which IGMP host query messages are sent by the interface, use the **igmp query-interval** command in interface configuration mode. To restore the default frequency, use the **no** form of this command.

igmp query-interval *seconds*

no igmp query-interval *seconds*

Syntax Description

seconds	Frequency, in seconds, at which to send IGMP host query messages. Valid values range from 1 to 3600. The default is 125 seconds.

Defaults

The default query interval is 125 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Multicast routers send host query messages to discover which multicast groups have members on the networks attached to the interface. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Host query messages are addressed to the all-hosts multicast group, which has an address of 224.0.0.1 TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages:

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Version 2, the designated router is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the **igmp query-timeout** command), it becomes the querier.

Caution Changing this value may severely impact multicast forwarding.

Examples

The following example changes the IGMP query interval to 120 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-max-response-time

To specify the maximum response time advertised in IGMP queries, use the **igmp query-max-response-time** command in interface configuration mode. To restore the default response time value, use the **no** form of this command.

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Valid values are from 1 to 25. The default value is 10 seconds.

Defaults

10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command is valid only when IGMP Version 2 or 3 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example changes the maximum query response time to 8 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-timeout

To configure the timeout period before the interface takes over as the querier after the previous querier has stopped querying, use the **igmp query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. Valid values are from 60 to 300 seconds. The default value is 255 seconds.

Defaults

The default query interval is 255 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command requires IGMP Version 2 or 3.

Examples

The following example configures the router to wait 200 seconds from the time it received the last query before it takes over as the querier for the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

igmp static-group

To configure the interface to be a statically connected member of the specified multicast group, use the **igmp static-group** command in interface configuration mode. To remove the static group entry, use the **no** form of this command.

igmp static-group *group*

no igmp static-group *group*

Syntax Description

group	IP multicast group address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When configured with the **igmp static-group** command, the security appliance interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the security appliance both accept and forward multicast packets for a speific multicast group, use the **igmp join-group** command. If the **igmp join-group** command is configured for the same group address as the **igmp static-group** command, the **igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Examples

The following example adds the selected interface to the multicast group 239.100.100.101:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

Related Commands

Command	Description
igmp join-group	Configures an interface to be a locally connected member of the specified group.

igmp version

To configure which version of IGMP the interface uses, use the **igmp version** command in interface configuration mode. To restore version to the default, use the **no** form of this command.

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.

Defaults

IGMP Version 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

All routers on the subnet must support the same version of IGMP. Hosts can have any IGMP version (1 or 2) and the security appliance will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2, such as the **igmp query-max-response-time** and **igmp query-timeout** commands.

Examples

The following example configures the selected interface to use IGMP Version 1:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

ignore-ipsec-keyusage

To suppress key-usage checking on IPsec client certificates, use the **ignore-ipsec-keyusage** command in configure-ca-trustpoint configuration mode. To resume key-usage checking, use the **no** form of this command.

ignore-ipsec-keyusage

no ignore-ipsec-keyusage

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Config-ca-trustpoint configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced as a safety measure and was deprecated at the same time. Note that future releases might not offer suppression of key-usage checking.

Usage Guidelines

Use of this command indicates that the values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates are not to be validated. This command ignores key-usage checking and is useful for non-compliant deployments.

Examples

The following example shows how to ignore the results of key-usage checking:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)#
hostname(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

ignore lsa mospf

To suppress the sending of syslog messages when the router receives LSA Type 6 MOSPF packets, use the **ignore lsa mospf** command in router configuration mode. To restore the sending of the syslog messages, use the **no** form of this command.

ignore lsa mospf

no ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Type 6 MOSPF packets are unsupported.

Examples

The following example cause LSA Type 6 MOSPF packets to be ignored:

```
hostname(config-router)# ignore lsa mospf
```

Related Commands

Command	Description
show running-config router ospf	Displays the OSPF router configuration.

ike-retry-count

To configure the maximum number of connection retry attempts a Cisco AnyConnect VPN Client using IKE should make before falling back to SSL to attempt the connection, use the **ike-retry-count** command in group-policy webvpn configuration mode, or username webvpn configuration mode. To remove this command from the configuration and reset the maximum number of retry attempts to the default value, use the **no** form of this command.

ike-retry-count {**none** | *value*}

no ike-retry-count [**none** | *value*]

Syntax Description

none	Specifies that no retry attempts are allowed.
value	Specify the maximum number of connection retry atttempts (1-10) for the Cisco AnyConnect VPN Client to perform after an inital connection failure.

Defaults

The default number of allowed retry attempts is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration	•	—	•	—	—
Username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced

Usage Guidelines

Use the **ike-retry-count** command to control the number of times that the Cisco AnyConnect VPN Client should attempt to connect using IKE. If the client fails to connect using IKE after the number of retries specified in this command, it falls back to SSL to attempt the connection. This value overrides any value that exists in the Cisco AnyConnect VPN Client.

Note To support fallback from IPSec to SSL, the **vpn-tunnel-protocol** command must be have with both the **svc** and **ipsec** arguments configured.

Examples

The following example sets the IKE retry count to 7 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-count 7
hostname(config-group-webvpn)#
```

The following example sets the IKE retry count to 9 for the username Finance:

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-count 9
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
group-policy	Creates or edits a group policy.
ike-retry-timeout	Specifies the number of seconds between IKE retry attempts.
username	Adds a user to the security appliance database.
vpn-tunnel-protocol	Configures a VPN tunnel type (IPSec, L2TP over IPSec, or WebVPN).
webvpn (group-policy or username mode)	Enters group-policy webvpn configuration mode or username webvpn configuration mode.

ike-retry-timeout

To configure the number of seconds between IKE retry attempts for a Cisco AnyConnect VPN Client, use the **ike-retry-timeout** command in group-policy webvpn or username webvpn configuration mode. To remove this command from the configuration and reset the timeout to the default value, use the **no** form of this command.

ike-retry-count *seconds*

no ike-retry-count

Syntax Description

seconds	Specify the number of seconds between IKE retry atttempts (1-3600) that the Cisco AnyConnect VPN Client performs after an inital connection failure.

Defaults

The default timeout is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced

Usage Guidelines

Use the **ike-retry-timeout** command to control the length of time between IKE retry attempts for the Cisco AnyConnect VPN Client. If the client fails to connect using IKE after the number of retries specified in the **ike-retry-count** command, it falls back to SSL to attempt the connection. This value overrides any value that exists in the Cisco AnyConnect VPN Client.

Note To support fallback from IPSec to SSL, the **vpn-tunnel-protocol** command must be have with both the **svc** and **ipsec** arguments configured.

Examples

The following example sets the IKE retry interval to 77seconds for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-timeout 77
hostname(config-group-webvpn)#
```

The following example sets the IKE retry count to 99 for the username Finance.:

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-timeout 9
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
group-policy	Creates or edits a group policy.
ike-retry-count	Specifies the maximum number of connection retry attempts a Cisco AnyConnect VPN Client using IKE should make before falling back to SSL to attempt the connection.
username	Adds a user to the security appliance database.
vpn-tunnel-protocol	Configures a VPN tunnel type (IPSec, L2TP over IPSec, or WebVPN).
webvpn (group-policy or username mode)	Enters group-policy webvpn mode or username webvpn mode.

im

To enable instant messaging over SIP, use the **im** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

im

no im

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable instant messaging over SIP in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# im
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

imap4s

To enter IMAP4S configuration mode, use the **imap4s** command in global configuration mode. To remove any commands entered in IMAP4S command mode, use the **no** form of this command.

IMAP4 is a client/server protocol in which your Internet server receives and holds e-mail for you. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. IMAP4S lets you receive e-mail over an SSL connection.

imap4s

no imap4s

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to enter IMAP4S configuration mode:

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
show running-config imap4s	Displays the running configuration for IMAP4S.

import webvpn customization

To load a customization object onto the flash device of the security appliance, enter the **import webvpn customization** command in privileged EXEC mode.

import webvpn customization *name URL*

Syntax Description

name	The name that identifies the customization object. Maximum 64 characters.
URL	Remote path to the source of the XML customization object. Maximum 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Make sure WebVPN is enabled on a security appliance interface before you enter the **import customization** command. To do so, enter the **show running-config** command.

The security appliance does the following when you import a customization object:

- Copies the customization object from the URL to the security appliance file system disk0:/csco_config/customization as MD5*name*.
- Performs a basic XML syntax check on the file. If it is invalid, the security appliance deletes the file.
- Checks that the file in index.ini contains the record MD5*name*. If not the security appliance adds MD5*name* to the file.
- Copies the MD5*name* file to RAMFS /csco_config/customization/ with as ramfs *name*.

Examples

The following example imports to the security appliance a customization object, *General.xml*, from the URL 209.165.201.22/customization and names it *custom1*.

```
hostname# import webvpn customization custom1 tftp://209.165.201.22/customization
/General.xml
```

```
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn customization	Removes the specified customization object from the flash device of the security appliance.
show import webvpn customization	Lists the customization objects present on the flash device of the security appliance.

import webvpn plug-in protocol

To install a plug-in onto the flash device of the security appliance, enter the **import webvpn plug-in protocol** command in privileged EXEC mode.

import webvpn plug-in protocol *protocol URL*

Syntax Description

protocol	• **rdp** The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. Cisco redistributes this plug-in without any changes. The web site containing the original is http://properjavardp.sourceforge.net/. • **ssh,telnet** The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. Cisco redistributes this plug-in without any changes. The web site containing the original is http://javassh.org/. **Caution** The **import webvpn plug-in protocol ssh,telnet** *URL* command installs *both* the SSH and Telnet plug-ins. Do *not* enter this command once for SSH and once for Telnet. When typing the **ssh,telnet** string, do *not* insert a space. Use the **revert webvpn plug-in protocol** command to remove any **import webvpn plug-in protocol** commands that deviate from these requirements. • **vnc** The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on. Cisco redistributes this plug-in without any changes. The web site containing the original is http://www.tightvnc.com/.
URL	Remote path to the source of the plug-in.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Before installing a plug-in:

- Make sure Clientless SSL VPN ("webvpn") is enabled on an interface on the security appliance. To do so, enter the **show running-config** command.
- Create a temporary directory named "plugins" on a local TFTP server (for example, with the hostname "local_tftp_server"), and download the plug-ins from the Cisco web site to the "plugins" directory. Enter the host name or address of the TFTP server and the path to the plug-in you need into the URL field of the **import webvpn plug-in protocol** command.

The security appliance does the following when you import a plug-in:

- Unpacks the jar file specified in the *URL*.
- Writes the file to the `csco-config/97/plugin` directory on the security appliance file system.
- Populates the drop-down menu next to the URL attributes in ASDM.
- Enables the plug-in for all future Clientless SSL VPN sessions, and adds a main menu option and an option to the drop-down menu next to the Address field of the portal page. Table 14-2 shows the changes to the main menu and address field of the portal page.

Table 14-2 Effects of Plug-ins on the Clientless SSL VPN Portal Page

Plug-in	Main Menu Option Added to Portal Page	Address Field Option Added to Portal Page
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

The security appliance does not retain the **import webvpn plug-in protocol** command in the configuration. Instead, it loads the contents of the `csco-config/97/plugin` directory automatically. A secondary security appliance obtains the plug-ins from the primary security appliance.

When the user in a Clientless SSL VPN session clicks the associated menu option on the portal page, the portal page displays a window to the interface and displays a help pane. The user can select the protocol displayed in the drop-down menu and enter the URL in the Address field to establish a connection.

Note The SSH client only supports SSH Version 1.0.

Some Java plug-ins may report a status of connected or online even when a session to the destination service is not set up. The open-source plug-in reports the status, not the security appliance.

To remove the respective **import webvpn plug-in protocol** command and disable support for the protocol, use the **revert webvpn plug-in protocol** command.

Examples

The following command adds Clientless SSL VPN support for RDP:

```
hostname# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!
```

import webvpn translation-table

To import a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **import webvpn translation-table** command from privileged EXEC mode.

import webvpn translation-table *translation_domain* **language** *language url*

Syntax Description

language	Specifies a language for the translation table. Enter the value for *language* in the manner expressed by your browser language options.
translation_domain	The functional area and associated messages visible to remote users. The usage guidelines section lists available translation domains.
url	Specifies the URL of the XML file used to create the customization object.

Defaults

This command has no default behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that is visible to remote users has its own translation domain and is specified by the *translation_domain* argument. The following table shows the translation domains and the functional areas translated.

Table 14-3 Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.

Translation Domain	Functional Areas Translated
banners	Banners displayed to remote users and messages when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the security appliance includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless users, the security appliance generates the **customization** and **url-list** translation domain templates dynamically and the template automatically reflects your changes to these functional areas.

Download the template for the translation domain using the **export webvpn translation-table** command, make changes to the messages, and use the **import webvpn translation-table** command to create the object. You can view available objects with the **show import webvpn translation-table** command.

Be sure to specify *language* in the manner expressed by your browser language options. For example, Microsoft Internet Explorer uses the abbreviation *zh* for the Chinese language. The translation table imported to the security appliance must also be named *zh*.

With the exception of the AnyConnect translation domain, a translation table has no affect, and messages are not translated until you create a customization object, identify a translation table to use in that object, and specify the customization for the group policy or user. Changes to the translation table for the AnyConnect domain are immediately visible to AnyConnect client users. See the **import webvpn customization** command for more information.

Examples

The following example imports a translation-table for the translation domain affecting the AnyConnect client user interface, and specifies the translation table is for the Chinese language. The **show import webvpn translation-table** command displays the new object:

```
hostname# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
```

```
Translation Tables:
zh AnyConnect
```

Related Commands

Command	Description
export webvpn translation-table	Exports a translation table.
import webvpn customization	Imports a customization object that references the translation table.
revert	Removes translation tables from flash.
show import webvpn translation-table	Displays available translation table templates and translation tables.

import webvpn url-list

To load a URL list onto the flash device of the security appliance, enter the **import webvpn url-list** command in privileged EXEC mode.

import webvpn url-list *name URL*

Syntax Description

name	The name that identifies the URL list. Maximum 64 characters.
URL	Remote path to the source of the URL list. Maximum 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
(8.0(2)	This command was introduced.

Usage Guidelines

Make sure WebVPN is enabled on a security appliance interface before you enter the **import url-list** command. To do so, enter the **show running-config** command.

The security appliance does the following when you import a URL list:

- Copies the URL list from the URL to the security appliance file system disk0:/csco_config/url-lists as *name on flash* = base 64*name*.
- Performs a basic XML syntax check on the file. If it is invalid, the security appliance deletes the file.
- Checks that the file in index.ini contains the record base 64*name*. If not the security appliance adds base 64*name* to the file.
- Copies the*name* file to RAMFS /csco_config/url-lists/ with ramfs name = *name*.

Examples

The following example imports to the security appliance a URL list, *NewList.xml*, from the URL 209.165.201.22/url-lists and names it *ABCList*.

```
hostname# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

Related Commands

Command	Description
revert webvpn url-list	Removes the specified URL list from the flash device of the security appliance.
show import webvpn url-list	Lists the URL lists present on the flash device of the security appliance.

import webvpn webcontent

To import content to flash memory that is visible to remote Clientless SSL VPN users, use the **import webvpn webcontent** command from privileged EXEC mode.

import webvpn webcontent *<destination url> <source url>*

Syntax Description

<source url>	The URL in the security appliance flash memory where the content resides. Maximum 64 characters.
<destination url>	The URL to export to. Maximum 255 characters.

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Content imported with the **webcontent** option is visible to remote Clientless users. This includes help content visible on the Clientless portal and logos used by customization objects that customize user screens.

Content imported to URLs with the path /+CSCOE+/ is visible only to authorized users.

Content imported to URLs with the path /+CSCOU+/ is visible to both unauthorized and authorized users.

For example, a corporate logo imported as /+CSCOU+/logo.gif could be used in a portal customization object and be visible on the logon page and the portal page. The same logo.gif file imported as /+CSCOE+/logo.gif would only be visible to remote users after they have logged in successfully.

Help content that appears on the various application screens must be imported to specific URLs. Table 14-4 shows the URLs and screen areas for the help content displayed for standard Clientless applications:

Table 14-4 Standard Clientless Applications

URL	Clientless Screen Area
/+CSCOE+/help/<*language*>/app-access-hlp.inc	Application Access
/+CSCOE+/help/<*language*>/file-access-hlp.inc	Browse Networks

Table 14-4 Standard Clientless Applications

URL	Clientless Screen Area
/+CSCOE+/help/<*language*>/net_access_hlp.html	AnyConnect Client
/+CSCOE+/help/<*language*>/web-access-help.inc	Web Access

Table 14-5 shows the URLs and screen areas for the help content displayed for optional plug-in Clientless applications:

Table 14-5 Plug-in Clientless Applications

URL	Clientless Screen Area
/+CSCOE+/help/<*language*>/ica-hlp.inc	MetaFrame Access
/+CSCOE+/help/<*language*>/rdp-hlp.inc	Terminal Servers
/+CSCOE+/help/<*language*>/ssh,telnet-hlp.inc	Telnet/SSH Servers
/+CSCOE+/help/<*language*>/vnc-hlp.inc	VNC Connections

<*language*> in the URL path is the language abbreviation you designate for the help content. The security appliance does not actually translate the file into the language you specify, but labels the file with the language abbreviation.

The following example imports the HTML file *application_access_help.html*, from a tftp server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
hostname#
```

Examples

The following example imports the HTML file *application_access_help.html*, from a tftp server at 209.165.200.225, to the URL that stores the Application Access help content in flash memory. The URL includes the abbrevation *en* for the English language:

```
hostname# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
hostname#
```

Related Commands

Command	Description
export webvpn webcontent	exports previously-imported content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

CHAPTER 15

inspect ctiqbe through inspect xdmcp Commands

inspect ctiqbe

To enable CTIQBE protocol inspection, use the **inspect ctiqbe** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable inspection, use the **no** form of this command.

inspect ctiqbe

no inspect ctiqbe

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced in 7.0. It replaces the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect ctiqbe** command enables CTIQBE protocol inspection, which supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the security appliance.

The Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI) are used by many Cisco VoIP applications. Computer Telephony Interface Quick Buffer Encoding (CTIQBE) is used by Cisco TAPI Service Provider (TSP) to communicate with Cisco CallManager.

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations using the **alias** command.
- Stateful Failover of CTIQBE calls is *not* supported.
- Using the **debug ctiqbe** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the security appliance, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.
- CTIQBE application inspection does *not* support CTIQBE messages fragmented in multiple TCP packets.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the security appliance, calls between these two phones will fail.
- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the **same port** of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect ctiqbe** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect ctiqbe** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect ctiqbe** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the CTIQBE inspection engine as shown in the following example, which creates a class map to match CTIQBE traffic on the default port (2748). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

To enable CTIQBE inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show conn	Displays the connection state for different connection types.
show ctiqbe	Displays information regarding the CTIQBE sessions established across the security appliance. Displays information about the media connections allocated by the CTIQBE inspection engine.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect dcerpc

To enable inspection of DCERPC traffic destined for the endpoint-mapper, use the **inspect dcerpc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

Syntax Description

map_name	(Optional) The name of the DCERPC map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **inspect dcerpc** command enables or disables application inspection for the DCERPC protocol.

Examples

The following example shows how to define a DCERPC inspection policy map with the timeout configured for DCERPC pinholes.

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc_map

hostname(config)# service-policy global-policy global
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
timeout pinhole	Configures the timeout for DCERPC pinholes and overrides the global system pinhole timeout.

inspect dns

To enable DNS inspection (if it has been previously disabled) or to configure DNS inspection parameters, use the **inspect dns** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable DNS inspection, use the **no** form of this command.

inspect dns [*map_name*]

no inspect dns [*map_name*]

Syntax Description

map_name	(Optional) The name of the DNS map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.
7.2(1)	This command was modified to allow configuration of additional DNS inspection parameters.

Usage Guidelines

DNS guard tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the security appliance. DNS guard also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

When DNS inspection is enabled, which it is the default, the security appliance performs the following additional tasks:

- Translates the DNS record based on the configuration completed using the **alias**, **static** and **nat** commands (DNS rewrite). Translation only applies to the A-record in the DNS reply. Therefore, reverse lookups, which request the PTR record, are not affected by DNS rewrite.

Note DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 65535 bytes). Reassembly is performed as necessary to verify that the packet length is less than the maximum length configured. The packet is dropped if it exceeds the maximum length.
- Enforces a domain-name length of 255 bytes and a label length of 63 bytes.
- Verifies the integrity of the domain-name referred to by the pointer if compression pointers are encountered in the DNS message.
- Checks to see if a compression pointer loop exists.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, if you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

How DNS Rewrite Works

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

DNS rewrite performs two functions:

- Translating a public address (the routable or “mapped” address) in a DNS reply to a private address (the “real” address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

As long as DNS inspection remains enabled, you can configure DNS rewrite using the **alias**, **static**, or **nat** commands. For details about the syntax and function of these commands, refer to the appropriate command page.

Examples

The following example shows how to set the maximum DNS message length:

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug dns	Enables debug information for DNS.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect esmtp

To enable SMTP application inspection or to change the ports to which the security appliance listens, use the **inspect esmtp** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

Syntax Description

map_name	(Optional) The name of the ESMTP map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the security appliance and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar in most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

The **inspect esmtp** command includes the functionality previously provided by the **fixup smtp** command, and provides additional support for some extended SMTP commands. Extended SMTP application inspection adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the security appliance supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions and are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

The **inspect esmtp** command changes the characters in the server SMTP banner to asterisks except for the “2”, “0”, “0” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

With SMTP inspection enabled, a Telnet session used for interactive SMTP waits for a valid command and the firewall esmtp state machine keeps the correct states for the session if the following rules are not observed: SMTP commands must be at least four characters in length; must be terminated with carriage return and line feed; and must wait for a response before issuing the next reply.

An SMTP server responds to client requests with numeric reply codes and optional human readable strings. SMTP application inspection controls and reduces the commands that the user can use as well as the messages that the server returns. SMTP inspection performs three primary tasks:

- Restricts SMTP requests to seven basic SMTP commands and eight extended commands.
- Monitors the SMTP command-response sequence.
- Generates an audit trail—Audit record 108002 is generated when invalid character embedded in the mail address is replaced. For more information, see RFC 821.

SMTP inspection monitors the command and response sequence for the following anomalous signatures:

- Truncated commands.
- Incorrect command termination (not terminated with <CR><LR>).
- If the PIPE signature is found as a parameter to a MAIL from or RCPT to command, the session is closed. It is not configurable by the user.
- Unexpected transition by the SMTP server.
- For unknown commands, the security appliance changes all the characters in the packet to X. In this case, the server will generate an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

Examples

You enable the SMTP inspection engine as shown in the following example, which creates a class map to match SMTP traffic on the default port (25). The service policy is then applied to the outside interface.

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

To enable SMTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug esmtp	Enables debug information for SMTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

inspect ftp

To configure the port for FTP inspection or to enable enhanced inspection, use the **inspect ftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

Syntax Description

map_name	The name of the FTP map.
strict	(Optional) Enables enhanced inspection of FTP traffic and forces compliance with RFC standards.

Caution Use caution when moving FTP to a higher port. For example, if you set the FTP port to 2021, all connections that initiate to port 2021 will have their data payload interpreted as FTP commands.

Defaults

The security appliance listens to port 21 for FTP by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated. The *map_name* option was added.

Usage Guidelines

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connections
- Tracks **ftp** command-response sequence
- Generates an audit trail
- NATs embedded IP addresses

Note Except for the banner, **inspect ftp** does not support FTP servers that segment FTP command or response.

FTP application inspection prepares secondary channels for FTP data transfer. The channels are allocated in response to a file upload, a file download, or a directory listing event and must be pre-negotiated. The port is negotiated through the PORT or PASV commands.

Note Only specify the port for the FTP control connection and not the data connection. The security appliance stateful inspection engine dynamically prepares the data connection as necessary.

Note If you disable FTP inspection engines with the **no inspect ftp** command, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

Using the strict Option

The **strict** option prevents web browsers from sending embedded commands in FTP requests. Each **ftp** command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The **strict** option only lets an FTP server generate the 227 command and only lets an FTP client generate the PORT command. The 227 and PORT commands are checked to ensure they do not appear in an error string.

To enable strict FTP application inspection for all interfaces, use the **global** parameter in place of **interface** command.

Caution The use of the **strict** option may break FTP clients that do not comply with the RFC standards.

If the **strict** option is enabled, each **ftp** command and response sequence is tracked for the following anomalous activity:

- Truncated command—Number of commas in the PORT and PASV reply command is checked to see if it is five. If it is not five, then the PORT command is assumed to be truncated and the TCP connection is closed.
- Incorrect command—Checks the **ftp** command to see if it ends with <CR><LF> characters, as required by the RFC. If it does not, the connection is closed.
- Size of RETR and STOR commands—These are checked against a fixed constant. If the size is greater, then an error message is logged and the connection is closed.
- Command spoofing—The PORT command should always be sent from the client. The TCP connection is denied if a PORT command is sent from the server.
- Reply spoofing—PASV reply command (227) should always be sent from the server. The TCP connection is denied if a PASV reply command is sent from the client. This prevents the security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- TCP stream editing.
- Invalid port negotiation—The negotiated dynamic port value is checked to see if it is less than 1024. As port numbers in the range from 1 to 1024 are reserved for well-known connections, if the negotiated port falls in this range, then the TCP connection is freed.
- Command pipelining—The number of characters present after the port numbers in the PORT and PASV reply command is cross checked with a constant value of 8. If it is more than 8, then the TCP connection is closed.
- The security appliance replaces the FTP server response to the SYST command with a series of Xs. to prevent the server from revealing its system type to FTP clients. To override this default behavior, use the **no mask-syst-reply** command in FTP map configuration mode.

Note To identify specific FTP commands that are not permitted to pass through the security appliance, identify an FTP map and use the **request-command deny** command. For details, see the **ftp-map** and the **request-command deny** command pages.

FTP Log Messages

FTP application inspection generates the following log messages:

- An Audit record 302002 is generated for each file that is retrieved or uploaded.
- The **ftp** command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

Examples

Before submitting a username and password, all FTP users are presented with a greeting banner. By default, this banner includes version information useful to hackers trying to identify weaknesses in a system. The following example shows how to mask this banner:

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
hostname(config-pmap-p)# exit
hostname(config-pmap)# exit
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
hostname(config-cmap)# exit
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy ftp-policy interface inside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.
request-command deny	Specifies FTP commands to disallow.
service-policy	Applies a policy map to one or more interfaces.

inspect gtp

To enable or disable GTP inspection or to define a GTP map for controlling GTP traffic or tunnels, use the **inspect gtp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to remove the command.

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

Note GTP inspection requires a special license. If you enter the **inspect gtp** command on a security appliance without the required license, the security appliance displays an error message.

Syntax Description

map_name	(Optional) Name for the GTP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

GTP is the tunnelling protocol for GPRS, and helps provide secure access over wireless networks. GPRS is a data network architecture that is designed to integrate with existing GSM networks. It offers mobile subscribers uninterrupted, packet-switched data services to corporate networks and the Internet. For an overview of GTP, refer to the "Applying Application Layer Protocol Inspection" chapter in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Use the **gtp-map** command to identify a specific map to use for defining the parameters for GTP. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **drop** and **rate-limit**. In addition to these actions, you can specify to **log** the event or not.

After defining the GTP map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

The well-known ports for GTP are as follows:

- 3386
- 2123

The following features are not supported in 7.0:

- NAT, PAT, Outside NAT, alias, and Policy NAT
- Ports other than 3386, 2123, and 2152
- Validating the tunneled IP packet and its contents

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect gtp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect gtp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect gtp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

The following example shows how to use access lists to identify GTP traffic, define a GTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

Note This example enables GTP inspection with the default values. To change the default values, refer to the **gtp-map** command page and to the command pages for each command that is entered from GTP map configuration mode.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
service-policy	Applies a policy map to one or more interfaces.
show service-policy inspect gtp	Shows that status and statistics of the **inspect gtp** policy.

inspect h323

To enable H.323 application inspection or to change the ports to which the security appliance listens, use the **inspect h323** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect h323 {**h225** | **ras**} [*map_name*]

no inspect h323 {**h225** | **ras**} [*map_name*]

Syntax Description

h225	Enables H.225 signalling inspection.
map_name	(Optional) The name of the H.323 map.
ras	Enables RAS inspection.

Defaults

The default port assignments are as follows:

- h323 h225 1720
- h323 ras 1718-1719

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect h323** command provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. The security appliance supports H.323 through Version 4, including the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the security appliance.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.

- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

How H.323 Works

The H.323 collection of protocols collectively may use up to two TCP connection and four to six UDP connections. FastStart uses only one TCP connection, and RAS uses a single UDP connection for registration, admissions, and status.

An H.323 client may initially establish a TCP connection to an H.323 server using TCP port 1720 to request Q.931 call setup. As part of the call setup process, the H.323 terminal supplies a port number to the client to use for an H.245 TCP connection. The H.245 connection is for call negotiation and media channel setup. In environments where H.323 gatekeeper is in use, the initial packet is transmitted using UDP.

H.323 inspection monitors the Q.931 TCP connection to determine the H.245 port number. If the H.323 terminals are not using FastStart, the security appliance dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Note The H.225 connection can also be dynamically allocated when using RAS.

Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP data streams. H.323 inspection inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. Real-Time Transport Protocol (RTP) uses the negotiated port number, while RTP Control Protocol (RTCP) uses the next higher port number.

The H.323 control channel handles H.225 and H.245 and H.323 RAS. H.323 inspection uses the following ports.

- 1718—UDP port used for gatekeeper discovery
- 1719—UDP port used for RAS and for gatekeeper discovery
- 1720—TCP Control Port

If the ACF message from the gatekeeper goes through the security appliance, a pinhole will be opened for the H.225 connection. The H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the security appliance opens an H.225 connection based on inspection of the ACF message. If | the security appliance does not see the ACF message, you might need to open an access list for the well-known H.323 port 1720 for the H.225 call signaling.

The security appliance dynamically allocates the H.245 channel after inspecting the H.225 messages and then hooks up to the H.245 channel to be fixed up as well. That means whatever H.245 messages pass through the security appliance pass through the H.245 application inspection, NATing embedded IP addresses and opening the negotiated media channels.

The H.323 ITU standard requires that a TPKT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as the H.225/H.245 message, the security appliance must remember the TPKT length to process/decode the messages properly. The security appliance keeps a data structure for each connection and that data structure contains the TPKT length for the next expected message.

If the security appliance needs to NAT any IP addresses, then it will have to change the checksum, the UUIE (user-user information element) length, and the TPKT, if included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, then the security appliance will proxy ACK that TPKT and append a new TPKT to the H.245 message with the new length.

Note The security appliance does not support TCP options in the Proxy ACK for the TPKT.

Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and will time out with the H.323 timeout as configured using the **timeout** command.

Limitations and Restrictions

The following are some of the known issues and limitations when using H.323 application inspection:

- Static PAT may not properly translate IP addresses embedded in optional fields within H.323 messages. If you experience this kind of problem, do not use static PAT with H.323.
- H.323 application inspection is not supported with NAT between same-security-level interfaces.
- It has been observed that when a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the security appliance.
- If you configure a network static where the network static is the same as a third-party netmask and address, then any outbound H.323 connection fails.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect h323** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect h323** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect h323** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the H.323 inspection engine as shown in the following example, which creates a class map to match H.323 traffic on the default port (1720). The service policy is then applied to the outside interface.

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

To enable H.323 inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
show h225	Displays information for H.225 sessions established across the security appliance.

Commands	Description
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout {**h225** | **h323**}	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

inspect http

To enable HTTP application inspection or to change the ports to which the security appliance listens, use the **inspect http command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect http [*map_name*]

no inspect http [*map_name*]

Syntax Description

map_name	(Optional) The name of the HTTP map.

Defaults

The default port for HTTP is 80.

Enhanced HTTP inspection is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect http** command protects against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions:

- Enhanced HTTP inspection
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

The latter two features are configured in conjunction with the **filter** command.

Enhanced HTTP inspection verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods, and comply with various other criteria. In many cases, you can configure these criteria and the system response when the criteria are not met. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

The criteria that you can apply to HTTP messages include the following:

- Does not include any method on a configurable list.

- Specific transfer encoding method or application type.
- HTTP transaction adheres to RFC specification.
- Message body size is within configurable limits.
- Request and response message header size is within a configurable limit.
- URI length is within a configurable limit.
- The content-type in the message body matches the header.
- The content-type in the response message matches the *accept-type* field in the request message.
- The content-type in the message is included in a predefined internal list.
- Message meets HTTP RFC format criteria.
- Presence or absence of selected supported applications.
- Presence or absence of selected encoding types.

Note The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

To enable enhanced HTTP inspection, enter the **inspect http** *http-map* command. The rules that this applies to HTTP traffic are defined by the specific HTTP map, which you configure by entering the **http-map** command and HTTP map configuration mode commands.

Note When you enable HTTP inspection with an HTTP map, strict HTTP inspection with the action reset and log is enabled by default. You can change the actions performed in response to inspection failure, but you cannot disable strict inspection as long as the HTTP map remains enabled.

Examples

The following example shows how to identify HTTP traffic, define an HTTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

This example causes the security appliance to reset the connection and create a syslog entry when it detects any traffic that contain the following:

- Messages less than 100 bytes or exceeding 2000 bytes

- Unsupported content types
- HTTP headers exceeding 100 bytes
- URIs exceeding 100 bytes

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
policy-map	Associates a class map with specific security actions.

inspect icmp

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode.

inspect icmp

no inspect icmp

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The ICMP inspection engine allows ICMP traffic to be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the security appliance in an ACL. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct

When ICMP inspection is disabled, which is the default configuration, ICMP echo reply messages are denied from a lower security interface to a higher security interface, even if it is in response to an ICMP echo request.

Examples

You enable the ICMP application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

To enable ICMP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect icmp error

To enable application inspection for ICMP error messages, use the **inspect icmp error** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode.

inspect icmp error

no inspect icmp error

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

Use the **inspect icmp error** command to create xlates for intermediate hops that send ICMP error messages, based on the static/NAT configuration. By default, the security appliance hides the IP addresses of intermediate hops. However, using the **inspect icmp error** command makes the intermediate hop IP addresses visible. The security appliance overwrites the packet with the translated IP addresses.

Cisco ASA 5500 Series Adaptive Security Appliance software uses the egress interface address as the source address when generating ICMP error messages for path MTU discovery or hop-by-hop discovery. If you enable application inspection for ICMP error messages using the **inspect icmp error** command, NAT is also independently applied to this source address.

When enabled, the ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the NAT IP is changed to the Client IP (Destination Address and Intermediate Hop Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet NAT IP is changed to the Client IP
  - Original packet NAT port is changed to the Client Port
  - Original packet IP checksum is recalculated

When an ICMP error message is retrieved, whether ICMP error inspection is enabled or not, the ICMP payload is scanned to retrieve the five-tuple (src ip , dest ip, src port, dest port, and ip protocol) from the original packet. A lookup is performed, using the retrieved five-tuple, to determine the original address of the client and to locate an existing session associated with the specific five-tuple. If the session is not found, the ICMP error message is dropped.

Examples

You enable the ICMP error application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

To enable ICMP error inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
inspect icmp	Enables or disables the ICMP inspection engine.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect ils

To enable ILS application inspection, use the **inspect ils command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ils

no inspect ils

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect ils** command provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

The security appliance supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the security appliance border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the **timeout** command.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment

ILS inspection has the following limitations:

- Referral requests and responses are not supported
- Users in multiple directories are not unified
- Single users having multiple identities in multiple directories cannot be recognized by NAT

Note Because H225 call signalling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP **timeout** command. By default, this interval is set at 60 minutes.

Examples

You enable the ILS inspection engine as shown in the following example, which creates a class map to match ILS traffic on the default port (389). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

To enable ILS inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug ils	Enables debug information for ILS.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect im

To enable inspection of IM traffic, use the **inspect im** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect im *map_name*

no inspect im *map_name*

Syntax Description

map_name	The name of the IM map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **inspect im** command enables or disables application inspection for the IM protocol.

Examples

The following example shows how to define an IM inspection policy map.

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
```

```
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect ipsec-pass-thru

To enable IPSec Pass Thru inspection, use the **inspect ipsec-pass-thru** command in class map configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

Syntax Description

map_name	(Optional) The name of the IPSec Pass Thru map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **inspect ipsec-pass-thru** command enables or disables application inspection. IPSec Pass Through application inspection provides convenient traversal of ESP (IP protocol 50) and/or AH (IP protocol 51) traffic associated with an IKE UDP port 500 connection. It avoids lengthy access list configuration to permit ESP and AH traffic and also provides security using timeout and max connections.

Use the IPSec Pass Through parameter map to identify a specific map to use for defining the parameters for the inspection. Use the **policy-map type inspect** command to access the parameters configuration, which lets you specify the restrictions for ESP or AH traffic. You can set the per client max connections and the idle timeout in parameters configuration.

Use **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces. The parameter map defined is enabled when used with the **inspect IPSec-pass-thru** command.

NAT and non-NAT traffic is permitted. However, PAT is not supported.

Note In ASA 7.0, the **inspect ipsec-pass-thru** command allowed only ESP traffic to pass through. To retain the same behavior in later versions, a default map that permits ESP is created and attached if the **inspect ipsec-pass-thru** command is specified without any arguments. This map can be seen in the output of the **show running-config all** command.

Examples

The following example shows how to use access lists to identify IKE traffic, define an IPSec Pass Thru parameter map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.
match protocol	Matches a specific IM protocol in an inspection class or policy map.

inspect mgcp

To enable MGCP application inspection or to change the ports to which the security appliance listens, use the **inspect mgcp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

Syntax Description

map_name	(Optional) The name of the MGCP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

To use MGCP, you usually need to configure at least two **inspect** commands: one for the port on which the gateway receives commands, and one for the port on which the Call Agent receives commands. Normally, a Call Agent sends commands to the default MGCP port for gateways, 2427, and a gateway sends commands to the default MGCP port for Call Agents, 2727.

MGCP is used for controlling media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses.

Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, broad-band wireless devices.

- Business gateways, that provide a traditional digital PBX interface or an integrated soft PBX interface to a Voice over IP network.

MGCP messages are transmitted over UDP. A response is sent back to the source address (IP address and UDP port number) of the command, but the response may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response.

Note MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the security appliance and allows MGCP end points to register with the call agent.

Use the **call-agent** and **gateway** commands in MGCP map configuration mode to configure the IP addresses of one or more call agents and gateways. Use the **command-queue** command in MGCP map configuration mode to specify the maximum number of MGCP commands that will be allowed in the command queue at one time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect mgcp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect mgcp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect mgcp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

The following example shows how to identify MGCP traffic, define a MGCP map, define a policy, and apply the policy to the outside interface. This creates a class map to match MGCP traffic on the default ports (2427 and 2727). The service policy is then applied to the outside interface.

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

This configuration allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117. The maximum number of MGCP commands that can be queued is 150.

To enable MGCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays information about MGCP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect mmp

To configure the MMP inspection engine, use the **inspect mmp** command in class configuration mode.

To remove MMP inspection, use the **no** form of this command.

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

Syntax Description

name	Species the TLS proxy instance name.
tls-proxy	Enables the TLS proxy for MMP inspection. The MMP protocol can additionally use the TCP transport; however, the CUMA client only supports the TLS transport. Therefore, the tls-proxy keyword is required to enable MMP inspection.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The ASA includes an inspection engine to validate the CUMA Mobile Multiplexing Protocol (MMP). MMP is a data transport protocol for transmitting data entities between CUMA clients and servers. Use the **inspect mmp** command when the ASA is deployed between CUMA clients and servers and inspection of MMP packets is required.

MMP inspection must be enabled with the TLS proxy because MMP traffic is transported only over a TLS connection.

Examples

The following example shows the use of the **inspect mmp** command to inspect MMP traffic:

```
hostname(config)# class-map mmp
hostname(config-cmap)# match port tcp eq 5443
hostname(config-cmap)# exit
hostname(config)# policy-map mmp-policy
hostname(config-pmap)# class mmp
hostname(config-pmap-c)# inspect mmp tls-proxy myproxy
```

```
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy mmp-policy interface outside
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.
debug mmp	Displays inspect MMP events.

inspect netbios

To enable NetBIOS application inspection or to change the ports to which the security appliance listens, use the **inspect netbios command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

Syntax Description

map_name	(Optional) The name of the NetBIOS map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect netbios** command enables or disables application inspection for the NetBIOS protocol.

Examples

The following example shows how to define a NetBIOS inspection policy map:

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect pptp

To enable PPTP application inspection or to change the ports to which the security appliance listens, use the **inspect pptp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect pptp

no inspect pptp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The Point-to-Point Tunneling Protocol (PPTP) is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE **[**RFC 2637**]** when negotiated over the PPTP TCP control channel. Port Address Translation is *not* performed for the unmodified version of GRE **[**RFC 1701, RFC 1702**]**.

Specifically, the security appliance inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network.

Examples

You enable the PPTP inspection engine as shown in the following example, which creates a class map to match PPTP traffic on the default port (1723). The service policy is then applied to the outside interface.

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

To enable PPTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug pptp	Enables debug information for PPTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect radius-accouting

To enable or disable RADIUS accounting inspection or to define a map for controlling traffic or tunnels, use the **inspect radius-accounting** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **no** form of this command to remove the command.

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

Syntax Description

map_name	(Optional) Name for the RADIUS accounting map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **radius-accounting** command to create a specific map to use for defining the parameters for RADIUS accounting. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **send**, **host**, **validate-attribute**, **enable gprs**, and **timeout users**. You can access these commands from **parameter** mode.

After defining the RADIUS accounting map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Note The **inspect radius-accounting** command can only be used with the **class-map type management** command.

Examples

The following example shows how to use access lists to identify RADIUS accounting traffic, define a RADIUS accounting map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# policy-map type inspect radius-accountin ra
```

Note This example enables RADIUS accounting inspection with the default values. To change the default values, refer to the **parameters** command page and to the command pages for each command that is entered from RADIUS accounting configuration mode.

Related Commands

Commands	Description
parameters	Defines the traffic class to which to apply security actions.
class-map type management	Lets you identify Layer 3 or 4 management traffic destined for the security appliance to which you want to apply actions.
show and **clear service-policy**	Lets you view and clear service policy settings.
debug inspect radius-accounting	Lets you debug RADIUS accounting inspection.
service-policy	Applies a policy map to one or more interfaces.

inspect rsh

To enable RSH application inspection or to change the ports to which the security appliance listens, use the **inspect rsh** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rsh

no inspect rsh

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

Examples

You enable the RSH inspection engine as shown in the following example, which creates a class map to match RSH traffic on the default port (514). The service policy is then applied to the outside interface.

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

To enable RSH inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect rtsp

To enable RTSP application inspection or to change the ports to which the security appliance listens, use the **inspect rtsp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

Syntax Description

map_name	(Optional) The name of the RTSP map.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect rtsp** command lets the security appliance pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

Note For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The security appliance only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that will be used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The security appliance parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the security appliance and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the security appliance does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the security appliance will need to keep state and remember the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the security appliance, add an **access-list** command statement from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options**>**Preferences**>**Transport**>**RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the security appliance, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the security appliance, add a **inspect rtsp** *port* command statement.

Restrictions and Limitations

The following restrictions apply to the **inspect rtsp** command:

- The security appliance does not support multicast RTSP or RTSP messages over UDP.
- The security appliance does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- With Cisco IP/TV, the number of NATs the security appliance performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.
- Media streams delivered over HTTP are not supported by RTSP application inspection. This is because RTSP inspection does not support HTTP cloaking (RTSP wrapped in HTTP).

Examples

You enable the RTSP inspection engine as shown in the following example, which creates a class map to match RTSP traffic on the default ports (554 and 8554). The service policy is then applied to the outside interface.

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-traffic
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

To enable RTSP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug rtsp	Enables debug information for RTSP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sip

To enable SIP application inspection or to change the ports to which the security appliance listens, use the **inspect sip** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the specified inspection session.
sip_map	Specifies a SIP policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the specified inspection session. The keyword tls-proxy cannot be used as a layer 7 policy map name.

Defaults

This command is enabled by default.

The default port assignment for SIP is 5060.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	The **tls-proxy** keyword was added.
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

SIP, as defined by the IETF, enables VoIP calls. SIP works with SDP for call signalling. SDP specifies the details of the media stream. Using SIP, the security appliance can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

Note If a remote endpoint tries to register with a SIP proxy on a network protected by the security appliance, the registration will fail under very specific conditions. These conditions are when PAT is configured for the remote endpoint, the SIP registrar server is on the outside network, and when the port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.

Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes, which will time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.

Note Only the Chat feature is currently supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

Technical Details

SIP inspection NATs the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL_ID/FROM/TO from the SIP payload that identifies the call, as well as the source and destination. Contained within this database are the media addresses and media ports that were contained in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. RTP/RTCP connections are opened between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message. However, subsequent messages may not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be NATed.

As a call is set up, the SIP session is considered in the “transient” state. This state remains until a Response message is received indicating the RTP media address and port on which the destination endpoint is listening. If there is a failure to receive the response messages within one minute, the signaling connection will be torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection will remain until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface will not traverse the security appliance, unless the security appliance configuration specifically allows it.

The media connections are torn down within two minutes after the connection becomes idle. This is, however, a configurable timeout and can be set for a shorter or longer period of time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect sip** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect sip** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect sip** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the SIP inspection engine as shown in the following example, which creates a class map to match SIP traffic on the default port (5060). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

To enable SIP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show sip	Displays information about SIP sessions established through the security appliance.
debug sip	Enables debug information for SIP.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect skinny

T o enable SCCP (Skinny) application inspection or to change the ports to which the security appliance listens, use the **inspect skinny** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

Syntax Description

phone-proxy *proxy_name*	Enables the phone proxy for the specified inspection session.
skinny_map	Specifies a skinny policy map name.
tls-proxy *proxy_name*	Enables TLS proxy for the specified inspection session. The keyword tls-proxy cannot be used as a layer 7 policy map name.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	The keyword **tls-proxy** was added.
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

Skinny (or Simple) Client Control Protocol (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323-compliant terminals. Application layer functions in the security appliance recognize SCCP Version 3.3. The functionality of the application layer software ensures that all SCCP signaling and media packets can traverse the security appliance by providing NAT of the SCCP Signaling packets.

There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2. The security appliance supports all versions through Version 3.3.2. The security appliance provides both PAT and NAT support for SCCP. PAT is necessary if you have limited numbers of global IP addresses for use by IP phones.

Normal traffic between the Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration.The security appliance also supports DHCP options 150 and 66, which allow the security appliance to send the location of a TFTP server to Cisco IP Phones and other DHCP clients. For more information, see the **dhcp-server** command.

Supporting Cisco IP Phones

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be **static** as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An identity static entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an access list to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an "identity" static entry. When using NAT, an identity static entry maps to the same IP address. When using PAT, it maps to the same IP address and port.

When the Cisco IP Phones are on a *higher* security interface compared to the TFTP server and Cisco CallManager, no access list or static entry is required to allow the Cisco IP Phones to initiate the connection.

Restrictions and Limitations

The following are limitations that apply to the current version of PAT and NAT support for SCCP:

- PAT will not work with configurations using the **alias** command.
- Outside NAT or PAT is **not** supported.

Note Stateful Failover of SCCP calls is now supported except for calls that are in the middle of call setup.

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones will fail because the security appliance currently does not support NAT or PAT for the file content transferred via TFTP. Although the security appliance does support NAT of TFTP messages, and opens a pinhole for the TFTP file to traverse the security appliance, the security appliance cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone's configuration files that are being transferred using TFTP during phone registration.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect skinny** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect skinny** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect skinny** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the SCCP inspection engine as shown in the following example, which creates a class map to match SCCP traffic on the default port (2000). The service policy is then applied to the outside interface.

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

To enable SCCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debug information.
show skinny	Displays information about SCCP sessions established through the security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

inspect snmp

To enable SNMP application inspection or to change the ports to which the security appliance listens, use the **inspect snmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect snmp *map_name*

no inspect snmp *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the inspect snmp command to enable SNMP inspection, using the settings configured with an SNMP map, which you create using the **snmp-map** command. Use the **deny version** command in SNMP map configuration mode to restrict SNMP traffic to a specific version of SNMP.

Earlier versions of SNMP are less secure so restricting SNMP traffic to Version 2 may be required by your security policy. To deny a specific version of SNMP, use the **deny version** command within an SNMP map, which you create using the **snmp-map** command. After configuring the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example identifies SNMP traffic, defines an SNMP map, defines a policy, enables SNMP inspection, and applies the policy to the outside interface:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
```

```
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

To enable strict snmp application inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sqlnet

To enable Oracle SQL*Net application inspection, use the **inspect sqlnet** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sqlnet

no inspect sqlnet

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 1521.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The SQL*Net protocol consists of different packet types that the security appliance handles to make the data stream appear consistent to the Oracle applications on either side of the security appliance.

The default port assignment for SQL*Net is 1521. This is the value used by Oracle for SQL*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL*Net inspection to a range of port numbers.

Note Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

The security appliance NATs all addresses and looks in the packets for all embedded ports to open for SQL*Net Version 1.

For SQL*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the security appliance, a flag will be set in the connection data structure to expect the Data or Redirect message that follows to be NATed and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be NATed and port connections will be opened.

Examples

You enable the SQL*Net inspection engine as shown in the following example, which creates a class map to match SQL*Net traffic on the default port (1521). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

To enable SQL*Net inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug sqlnet	Enables debug information for SQL*Net.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*net.

inspect sunrpc

To enable Sun RPC application inspection or to change the ports to which the security appliance listens, use the **inspect sunrpc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sunrpc

no inspect sunrpc

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

To enable Sun RPC application inspection or to change the ports to which the security appliance listens, use the **inspect sunrpc** command in policy map class configuration mode, which is accessible by using the **class** command within policy map configuration mode. To remove the configuration, use the **no** form of this command.

The **inspect sunrpc** command enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port on the system. When a client attempts to access an Sun RPC service on a server, it must find out which port that service is running on. It does this by querying the portmapper process on the well-known port of 111.

The client sends the Sun RPC program number of the service, and gets back the port number. From this point on, the client program sends its Sun RPC queries to that new port. When a server sends out a reply, the security appliance intercepts this packet and opens both embryonic TCP and UDP connections on that port.

Note NAT or PAT of Sun RPC payload information is not supported.

Examples

You enable the RPC inspection engine as shown in the following example, which creates a class map to match RPC traffic on the default port (111). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

To enable RPC inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
clear configure sunrpc_server	Removes the configuration performed using the **sunrpc-server** command.
clear sunrpc-server active	Clears the pinholes that are opened by Sun RPC application inspection for specific services, such as NFS or NIS.
show running-config sunrpc-server	Displays the information about the Sun RPC service table configuration.
sunrpc-server	Allows pinholes to be created with a specified timeout for Sun RPC services, such as NFS or NIS.
show sunrpc-server active	Displays the pinholes open for Sun RPC services.

inspect tftp

To disable TFTP application inspection, or to enable it if it has been previously disabled, use the **inspect tftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect tftp

no inspect tftp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 69.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

Trivial File Transfer Protocol (TFTP), described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

Examples

You enable the TFTP inspection engine as shown in the following example, which creates a class map to match TFTP traffic on the default port (69). The service policy is then applied to the outside interface.

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

To enable TFTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect waas

To enable WAAS application inspection, use the **inspect waas** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect waas

no inspect waas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WAAS application inspection:

```
hostname(config-pmap-c)# inspect waas
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect waas

To enable WAAS application inspection, use the **inspect waas** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect waas

no inspect waas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WAAS application inspection:

```
hostname(config-pmap-c)# inspect waas
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect xdmcp

To enable XDMCP application inspection or to change the ports to which the security appliance listens, use the **inspect xdmcp command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect xdmcp

no inspect xdmcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect xdmcp** command enables or disables application inspection for the XDMCP protocol.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the security appliance must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the security appliance. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where *n* is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the security appliance can NAT if needed. XDCMP inspection does not support PAT.

Examples

You enable the XDMCP inspection engine as shown in the following example, which creates a class map to match XDMCP traffic on the default port (177). The service policy is then applied to the outside interface.

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

To enable XDMCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug xdmcp	Enables debug information for XDMCP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

CHAPTER 16

intercept-dhcp through issuer-name Commands

intercept-dhcp

To enable DHCP Intercept, use the **intercept-dhcp enable** command in group-policy configuration mode. To disable DHCP Intercept, use the **intercept-dhcp disable** command. To remove the intercept-dhcp attribute from the running configuration and allow the users to inherit a DHCP Intercept configuration from the default or other group policy, use the **no intercept-dhcp** command.

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

Syntax Description

disable	Disables DHCP Intercept.
enable	Enables DHCP Intercept.
netmask	Provides the subnet mask for the tunnel IP address.

Defaults

DHCP Intercept is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the security appliance limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

DHCP Intercept lets Microsoft XP clients use split-tunneling with the security appliance. The security appliance replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous.

Examples

The following example shows how to set DHCP Intercepts for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

interface

To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode. In interface configuration mode, you can configure hardware settings (for physical interfaces), assign a name, assign a VLAN, assign an IP address, and configure many other settings, depending on the type of interface and the security context mode.

In multiple context mode, you might need to specify the mapped name if one was assigned using the **allocate-interface** command.

All models can configure parameters for physical interfaces.

All models except for those with a built-in switch, such as the ASA 5505 adaptive security appliance, can create logical redundant interfaces.

All models except for those with a built-in switch, such as the ASA 5505 adaptive security appliance, can create logical subinterfaces that are assigned to a VLAN. Models with a built-in switch include switch ports (called physical interfaces in this command) that you can assign to a VLAN interface; in this case, you do not create a subinterface for the VLAN, but instead create a VLAN interface independent of any physical interfaces. You can then assign one or more physical interfaces to the VLAN interface.

To remove a redundant interface, subinterface, or VLAN interface, use the **no** form of this command; you cannot remove a physical interface or a mapped interface.

For physical interfaces (for all models):

interface *physical_interface*

For redundant interfaces (not available for models with a built-in switch):

interface redundant *number*

no interface redundant *number*

For subinterfaces (not available for models with a built-in switch):

interface {*physical_interface* | **redundant** *number*}**.***subinterface*

no interface {*physical_interface* | **redundant** *number*}**.***subinterface*

For VLAN interfaces (for models with a built-in switch):

interface vlan *number*

no interface vlan *number*

For multiple context mode when a mapped name is assigned:

interface *mapped_name*

Syntax Description

mapped_name	In multiple context mode, specifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Specifies the physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional. The physical interface types include the following: • **ethernet** • **gigabitethernet** • **management** (for ASA 5500 only) For the PIX 500 series security appliance, enter the type followed by the port number, for example, **ethernet0**. For the ASA 5500 series adaptive security appliance, enter the type followed by slot/port, for example, **gigabitethernet 0/1**. Interfaces that are built into the chassis are assigned to slot 0, while interfaces on the 4GE SSM (or a built-in 4GE SSM) are assigned to slot 1. The management interface is a Fast Ethernet interface designed for management traffic only, and is specified as **management 0/0**. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode. See the hardware documentation that came with your model to identify the interface type, slot, and port number.
redundant *number*	Specifies a logical redundant interface, where *number* is between 1 and 8. A redundant interface pairs an active and a standby physical interface (see the **member-interface** command). When the active interface fails, the standby interface becomes active and starts passing traffic. All security appliance configuration refers to the logical redundant interface instead of the member physical interfaces. A space between **redundant** and the ID is optional.
subinterface	Specifies an integer between 1 and 4294967293 designating a logical subinterface. The maximum number of subinterfaces varies depending on your security appliance model. Subinterfaces are not available for models with a built-in switch, such as the ASA 5505 adaptive security appliance. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for the maximum subinterfaces (or VLANs) per platform. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk.
vlan *number*	For models with a built-in switch, specifies a VLAN ID number between 1 and 4090.

Defaults

By default, the security appliance automatically generates **interface** commands for all physical interfaces.

In multiple context mode, the security appliance automatically generates **interface** commands for all interfaces allocated to the context using the **allocate-interface** command.

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified to allow for new subinterface naming conventions and to change arguments to be separate commands under interface configuration mode.
7.2(1)	The **interface vlan** command was added to support a built-in switch, as on the ASA 5505 adaptive security appliance.
8.0(2)	The **interface redundant** command was added.

Usage Guidelines

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For subinterfaces, also configure the **vlan** command. For switch physical interfaces, assign the physical interface to the VLAN interface using the **switchport access vlan** command.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly using the **security-level** command, then the security appliance sets the security level to 100.

Multiple Context Mode Guidelines

- Configure the context interfaces from within each context.
- Configure context interfaces that you already assigned to the context in the system configuration. Other interfaces are not available.

- Configure Ethernet settings, redundant interfaces, and subinterfaces in the system configuration. No other configuration is available. The exception is for failover interfaces, which are configured in the system configuration. Do not configure failover interfaces with this command.

Transparent Firewall Guidelines

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliances, you can use the Management 0/0 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

Subinterface Guidelines

- Maximum Subinterfaces—To determine how many subinterfaces are allowed for your platform, see the license information in the *Cisco ASA 5500 Series Configuration Guide using the CLI*.
- Preventing Untagged Packets on the Physical Interface—If you use subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. This property is also true for the active physical interface in a redundant interface pair. Because the physical or redundant interface must be enabled for the subinterface to pass traffic, ensure that the physical or redundant interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical or redundant interface pass untagged packets, you can configure the **nameif** command as usual.

Redundant Interface Guidelines

- Failover Guidelines:
  - If you want to use a redundant interface for the failover or state link, then you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.
  - If you use a redundant interface for the failover or state link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
  - You can monitor redundant interfaces for failover using the **monitor-interface** command; be sure to reference the logical redundant interface name.
  - When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.
- Redundant Interface MAC Address—The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the **mac-address** command or the **mac-address auto** command). When the active interface fails over to the standby, the same MAC address is maintained so traffic is not disrupted.
- Physical Interface Guidelines—Follow these guidelines when adding member interfaces:
  - Both member interfaces must be of the same physical type. For example, both must be Ethernet.
  - You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.

Caution If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

- The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters such as **speed** and **duplex** commands, the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.
- If you shut down the active interface, then the standby interface becomes active.

Built-in Switch Guidelines

For models with a built-in switch, you configure physical parameters and switch parameters (including the VLAN assignment) for the physical interfaces only. You configure all other parameters for the VLAN interface.

For the ASA 5505 adaptive security appliance in transparent firewall mode, you can configure two active VLANs in the Base license and three active VLANs in the Security Plus license, one of which must be for failover. In routed mode, you can configure up to three active VLANs with the Base license, and up to five active VLANs with the Security Plus license. An active VLAN is a VLAN with a **nameif** command configured. You can configure as many VLANs as you want as long as you limit the number of active VLANs to comply with your license. With the Base license, the third VLAN can only be configured to initiate traffic to one other VLAN. You limit the third VLAN using the **no forward interface** command. With the Security Plus license, you can configure three VLAN interfaces for normal traffic, one VLAN interface for failover, and one VLAN interface as a backup link to your ISP. However, the failover VLAN interface is not configured using the **interface vlan** command. After you assign a physical interface to the failover VLAN ID, use the **failover lan** commands to create and configure the VLAN interface. The backup link to the ISP must be identified by the **backup interface** command under the primary VLAN configuration. This interface does not pass through traffic unless the primary interface fails. See the **backup interface** command for more information.

Management-Only Interface

The ASA 5510 and higher adaptive security appliances include a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliances, you can use the Management 0/0 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

Examples

The following example configures parameters for the physical interface in single mode:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example configures parameters for a subinterface in single mode:

```
hostname(config)# interface gigabitethernet0/1.1
```

```
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work inteface.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

The following example configures five VLAN interfaces, including the failover interface which is configured separately using the **failover lan** command:

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

The following example creates two redundant interfaces:

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
```

```
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
member-interface	Assigns interfaces to a redundant interface.
clear interface	Clears counters for the **show interface** command.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN to a subinterface.

interface (vpn load-balancing)

To specify a non-default public or private interface for VPN load-balancing in the VPN load-balancing virtual cluster, use the **interface** command in vpn load-balancing mode. To remove the interface specification and revert to thte default interface, use the **no** form of this command.

interface {**lbprivate** | **lbpublic}** *interface-name*]

no interface {**lbprivate** | **lbpublic**}

Syntax Description

interface-name	The name of the interface to be configured as the public or private interface for the VPN load-balancing cluster.
lbprivate	Specifies that this command configures the private interface for VPN load-balancing.
lbpublic	Specifies that this command configures the public interface for VPN load-balancing.

Defaults

If you omit the **interface** command, the **lbprivate** interface defaults to **inside**, and the **lbpublic** interface defaults to **outside**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have first used the **vpn load-balancing** command to enter vpn load-balancing mode.

You must also have previously used the **interface**, **ip address** and **nameif** commands to configure and assign a name to the interface that you are specifying in this command.

The no form of this command reverts the interface to its default.

Examples

The following is an example of a **vpn load-balancing** command sequence that includes an **interface** command that specifies the public interface of the cluster as “test” one that reverts the private interface of the cluster to the default (inside):

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
```

```
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **interface-policy** command in failover group configuration mode. To restore the default values, use the **no** form of this command.

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

If the **failover interface-policy** command is configured for the unit, then the default for the **interface-policy** failover group command assumes that value. If not, then *num* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other security appliance is functioning properly, the security appliance will mark itself as failed and a failover may occur (if the active security appliance is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Examples

The following partial example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover interface-policy	Configures the interface monitoring policy.
monitor-interface	Specifies the interfaces being monitored for failover.

internal-password

To display an additional password field on the clientless SSL VPN portal page, use the **internal-password** command in webvpn configuration mode. This additional password is used by the security appliance to authenticate users to file servers for which SSO is allowed.

To disable the ability to use an internal password, use the **no** version of the command.

internal-password enable

no internal password

Syntax Description

enable	Enables use of an internal password.

Defaults

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If enabled, end users type a second password when logging in to a clientless SSL VPN session. The Clientless SSL VPN server sends an SSO authentication request, including the username and password, to the authenticating server using HTTPS. If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the Clientless SSL VPN server. This cookie is kept on the security appliance on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

The internal password feature is useful if you require that the internal password be different from the SSL VPN password. In particular, you can use one-time passwords for authentication to the security appliance, and another password for internal sites.

Examples

The following example shows how to enable the internal password:

```
hostname(config)# webvpn
hostname(config-webvpn)# internal password enable
hostname(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn configuration mode, which lets you configure attributes for clientless SSLVPN connections.

interval maximum

To configure the maximum interval between update attempts by a DDNS update method, use the **interval** command in DDNS-update-method mode. To remove an interval for a DDNS update method from the running configuration, use the **no** form of this command.

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

Syntax Description

days	Specifies the number of days between update attempts with a range of 0 to 364.
hours	Specifies the number of hours between update attempts with a range of 0 to 23.
minutes	Specifies the number of minutes between update attempts with a range of 0 to 59.
seconds	Specifies the number of seconds between update attempts with a range of 0 to 59.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
DDNS-update-method configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The days, hours, minutes, and seconds are added together to arrive at the total interval.

Examples

The following example configures a method called ddns-2 to attempt an update every 3 minutes and 15 seconds:

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# interval maximum 0 0 3 15
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform dynamic DNS updates.

invalid-ack

To set the action for packets with an invalid ACK, use the **invalid-ack** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

invalid-ack {**allow** | **drop**}

no invalid-ack

Syntax Description

allow	Allows packets with an invalid ACK.
drop	Drops packets with an invalid ACK.

Defaults

The default action is to drop packets with an invalid ACK.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **invalid-ack**—In tcp-map configuration mode, you can enter the **invalid-ack** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

You might see invalid ACKs in the following instances:

- In the TCP connection SYN-ACK-received status, if the ACK number of a received TCP packet is not exactly same as the sequence number of the next TCP packet sending out, it is an invalid ACK.

- Whenever the ACK number of a received TCP packet is greater than the sequence number of the next TCP packet sending out, it is an invalid ACK.

Note TCP packets with an invalid ACK are automatically allowed for WAAS connections.

Examples

The following example sets the security appliance to allow packets with an invalid ACK:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# invalid-ack allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

ip address

To set the IP address for an interface (in routed mode) or for the management address (transparent mode), use the **ip address** command. For routed mode, enter this command in interface configuration mode. In transparent mode, enter this command in global configuration mode. To remove the IP address, use the **no** form of this command. This command also sets the standby address for failover.

ip address *ip_address* [*mask*] [**standby** *ip_address*]

no ip address [*ip_address*]

Syntax Description

ip_address	The IP address for the interface (routed mode) or the management IP address (transparent mode).
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
standby *ip_address*	(Optional) The IP address for the standby unit for failover.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is to set the management IP address. This address is required because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

The following example sets the management address and standby address of a transparent firewall:

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
show ip address	Shows the IP address assigned to an interface.

ip address dhcp

To use DHCP to obtain an IP address for an interface, use the **ip address dhcp** command in interface configuration mode. To disable the DHCP client for this interface, use the **no** form of this command.

ip address dhcp [**setroute**]

no ip address dhcp

Syntax Description

setroute	(Optional) Allows the security appliance to use the default route supplied by the DHCP server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from a global configuration command to an interface configuration mode command. You can also enable this command on any interface, instead of only the outside interface.

Usage Guidelines

Reenter this command to reset the DHCP lease and request a new lease.

If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

Note The security appliance rejects any leases that have a timeout of less than 32 seconds.

Examples

The following example enables DHCP on the gigabitethernet0/1 interface:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
show ip address dhcp	Shows the IP address obtained from the DHCP server.

ip address pppoe

To enable PPPoE, use the **ip address pppoe** command in interface configuration mode. To disable PPPoE, use the **no** form of this command.

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]

no ip address [*ip_address* [*mask*]] **pppoe**

Syntax Description

ip_address	Manually sets the IP address instead of receiving an address from the PPPoE server.
mask	Specifies the subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
setroute	Lets the security appliance use the default route supplied by the PPPoE server. If the PPPoE server does not send a default route, the security appliance creates a default route with the address of the access concentrator as the gateway.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

PPPoE combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.

Before you set the IP address using PPPoE, configure the **vpdn** commands to set the username, password, and authentication protocol. If you enable this command on more than one interface, for example for a backup link to your ISP, then you can assign each interface to a different VPDN group if necessary using the **pppoe client vpdn group** command.

The maximum transmission unit (MTU) size is automatically set to 1492 bytes, which is the correct value to allow PPPoE transmission within an Ethernet frame.

Reenter this command to reset and restart the PPPoE session.

You cannot set this command at the same time as the **ip address** command or the **ip address dhcp** command.

Examples

The following example enables PPPoE on the Gigabitethernet 0/1 interface:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address pppoe
hostname(config-if)# no shutdown
```

The following example manually sets the IP address for a PPPoE interface:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for an interface.
pppoe client vpdn group	Assigns this interface to a particular VPDN group.
show ip address pppoe	Shows the IP address obtained from the PPPoE server.
vpdn group	Creates a

ip-address-privacy

To enable IP address privacy, use the **ip-address-privacy** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

ip-address-privacy

no ip-address-privacy

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable IP address privacy over SIP in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ip-address-privacy
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

ip audit attack

To set the default actions for packets that match an attack signature, use the **ip audit attack** command in global configuration mode. To restore the default action (to reset the connection), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to send and alarm.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an attack signature. The audit policy for the inside interface overrides this default to be alarm only, while the policy for the outside interface uses the default setting set with the **ip audit attack** command.

```
hostname(config)# ip audit attack action alarm reset
```

```
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

ip audit info

To set the default actions for packets that match an informational signature, use the **ip audit info** command in global configuration mode. To restore the default action (to generate an alarm), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to generate an alarm.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an informational signature. The audit policy for the inside interface overrides this default to be alarm and drop, while the policy for the outside interface uses the default setting set with the **ip audit info** command.

```
hostname(config)# ip audit info action alarm reset
```

```
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit info	Shows the configuration for the **ip audit info** command.

ip audit interface

To assign an audit policy to an interface, use the **ip audit interface** command in global configuration mode. To remove the policy from the interface, use the **no** form of this command.

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

Syntax Description

interface_name	Specifies the interface name.
policy_name	The name of the policy you added with the **ip audit name** command. You can assign an **info** policy and an **attack** policy to each interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example applies audit policies to the inside and outside interfaces:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.

Command	Description
ip audit signature	Disables a signature.
show running-config ip audit interface	Shows the configuration for the **ip audit interface** command.

ip audit name

To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the **ip audit name** command in global configuration mode. Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. To remove the policy, use the **no** form of this command.

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

Syntax Description

action	(Optional) Specifies that you are defining a set of actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, then the security appliance uses the default action set by the **ip audit attack** and **ip audit info** commands.
alarm	(Optional) Generates a system message showing that a packet matched a signature.
attack	Creates an audit policy for attack signatures; the packet might be part of an attack on your network, such as a DoS attack or illegal FTP commands.
drop	(Optional) Drops the packet.
info	Creates an audit policy for informational signatures; the packet is not currently attacking your network, but could be part of an information-gathering activity, such as a port sweep.
name	Sets the name of the policy.
reset	(Optional) Drops the packet and closes the connection.

Defaults

If you do not change the default actions using the **ip audit attack** and **ip audit info** commands, then the default action for attack signatures and informational signatures is to generate an alarm.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To apply the policy, assign it to an interface using the **ip audit interface** command. You can assign an **info** policy and an **attack** policy to each interface.

For a list of signatures, see the **ip audit signature** command.

If traffic matches a signature, and you want to take action against that traffic, use the **shun** command to prevent new connections from the offending host and to disallow packets from any existing connection.

Examples

The following example sets an audit policy for the inside interface to generate an alarm for attack and informational signatures, while the policy for the outside interface resets the connection for attacks:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
shun	Blocks packets with a specific source and destination address.

ip audit signature

To disable a signature for an audit policy, use the **ip audit signature** command in global configuration mode. To reenable the signature, use the **no** form of this command. You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms.

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

Syntax Description

signature_number	Specifies the signature number to disable. See Table 16-1 for a list of supported signatures.
disable	Disables the signature.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Table 16-1 lists supported signatures and system message numbers.

Table 16-1 Signature IDs and System Message Numbers

Signature ID	Message Number	Signature Title	Signature Type	Description
1000	400000	IP options-Bad Option List	Informational	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001	400001	IP options-Record Packet Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
1002	400002	IP options-Timestamp	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003	400003	IP options-Security	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004	400004	IP options-Loose Source Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005	400005	IP options-SATNET ID	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006	400006	IP options-Strict Source Route	Informational	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100	400007	IP Fragment Attack	Attack	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
1102	400008	IP Impossible Packet	Attack	Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1103	400009	IP Overlapping Fragments (Teardrop)	Attack	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.
2000	400010	ICMP Echo Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
2001	400011	ICMP Host Unreachable	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2002	400012	ICMP Source Quench	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
2003	400013	ICMP Redirect	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004	400014	ICMP Echo Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005	400015	ICMP Time Exceeded for a Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006	400016	ICMP Parameter Problem on Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
2007	400017	ICMP Timestamp Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
2008	400018	ICMP Timestamp Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009	400019	ICMP Information Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010	400020	ICMP Information Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011	400021	ICMP Address Mask Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012	400022	ICMP Address Mask Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2150	400023	Fragmented ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.
2151	400024	Large ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
2154	400025	Ping of Death Attack	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3040	400026	TCP NULL flags	Attack	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3041	400027	TCP SYN+FIN flags	Attack	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3042	400028	TCP FIN only flags	Attack	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3153	400029	FTP Improper Address Specified	Informational	Triggers if a port command is issued with an address that is not the same as the requesting host.
3154	400030	FTP Improper Port Specified	Informational	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
4050	400031	UDP Bomb attack	Attack	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
4051	400032	UDP Snork attack	Attack	Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052	400033	UDP Chargen DoS attack	Attack	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
6050	400034	DNS HINFO Request	Informational	Triggers on an attempt to access HINFO records from a DNS server.

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6051	400035	DNS Zone Transfer	Informational	Triggers on normal DNS zone transfers, in which the source port is 53.
6052	400036	DNS Zone Transfer from High Port	Informational	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053	400037	DNS Request for All Records	Informational	Triggers on a DNS request for all records.
6100	400038	RPC Port Registration	Informational	Triggers when attempts are made to register new RPC services on a target host.
6101	400039	RPC Port Unregistration	Informational	Triggers when attempts are made to unregister existing RPC services on a target host.
6102	400040	RPC Dump	Informational	Triggers when an RPC dump request is issued to a target host.
6103	400041	Proxied RPC Request	Attack	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153	400045	ypupdated (YP update daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155	400047	mountd (mount daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6180	400049	rexd (remote execution daemon) Attempt	Informational	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
6190	400050	statd Buffer Overflow	Attack	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Examples

The following example disables signature 6100:

```
hostname(config)# ip audit signature 6100 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit signature	Shows the configuration for the **ip audit signature** command.

ip-comp

To enable LZS IP compression, use the **ip-comp enable** command in group-policy configuration mode. To disable IP compression, use the **ip-comp disable** command.

To remove the **ip-comp** attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value from another group policy.

ip-comp {**enable** | **disable**}

no ip-comp

Syntax Description

disable	Disables IP compression.
enable	Enables IP compression.

Defaults

IP compression is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.

Caution Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the security appliance. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

Examples

The following example shows how to enable IP compression for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip local pool

To configure IP address pools to be used for VPN remote access tunnels, use the **ip local pool** command in global configuration mode. To delete address pools, use the **no** form of this command.

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

Syntax Description

first-address	Specifies the starting address in the range of IP addresses.
last-address	Specifies the final address in the range of IP addresses.
mask *mask*	(Optional) Specifies a subnet mask for the pool of addresses.
poolname	Specifies the name of the IP address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must supply the mask value when the IP addresses assigned to VPN clients belong to a non-standard network and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets fall under the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

Examples

The following example configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools.
show running-config ip local pool	Displays the ip pool configuration. To specify a specific IP address pool, include the name in the command.

ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode. To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for IP Phone Bypass from another group policy.

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. If enabled, secure unit authentication remains in effect.

ip-phone-bypass {**enable | disable**}

no ip-phone-bypass

Syntax Description

disable	Disables IP Phone Bypass.
enable	Enables IP Phone Bypass.

Defaults

IP Phone Bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You need to configure IP Phone Bypass only if you have enabled user authentication.

Examples

The following example shows how to enable IP Phone Bypass. for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

Related Commands

Command	Description
user-authentication	Requires users behind a hardware client to identify themselves to the security appliance before connecting.

ips

The ASA 5500 series adaptive security appliance supports the AIP SSM, which runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. To divert traffic from the adaptive security appliance to the AIP SSM for inspection, use the **ips** command in class configuration mode. To remove this command, use the **no** form of this command.

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}]

Syntax Description

fail-close	Blocks traffic if the AIP SSM fails.
fail-open	Permits traffic if the AIP SSM fails.
inline	Directs packets to the AIP SSM; the packet might be dropped as a result of IPS operation.
promiscuous	Duplicates packets for the AIP SSM; the original packet cannot be dropped by the AIP SSM.
sensor {*sensor_name* | *mapped_name*}	Sets the virtual sensor name for this traffic. If you use virtual sensors on the AIP SSM (using Version 6.0 or above), you can specify a sensor name using this argument. To see available sensor names, enter the **ips ... sensor ?** command. Available sensors are listed. You can also use the **show ips** command. If you use multiple context mode on the adaptive security appliance, you can only specify sensors that you assigned to the context (see the **allocate-ips** command). Use the *mapped_name* if configured in the context. If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM. If you enter a name that does not yet exist on the AIP SSM, you get an error, and the command is rejected.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	Virtual sensor support was added.

Usage Guidelines

Before or after you configure the **ips** command on the adaptive security appliance, configure the security policy on the AIP SSM. You can either session to the AIP SSM from the adaptive security appliance (the **session** command) or you can connect directly to the AIP SSM using SSH or Telnet on its mangement interface. Alternatively, you can use ASDM. For more information about configuring the AIP SSM, see *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

To configure the **ips** command, you must first configure the **class-map** command, **policy-map** command, and the **class** command.

The AIP SSM runs a separate application from the adaptive security appliance. It is, however, integrated into the adaptive security appliance traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you apply the **ips** command for a class of traffic on the adaptive security appliance, traffic flows through the adaptive security appliance and the AIP SSM in the following way:

1. Traffic enters the adaptive security appliance.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane (using the **inline** keyword; See the **promiscuous** keyword for information about only sending a copy of the traffic to the AIP SSM).
4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the adaptive security appliance over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the adaptive security appliance.

Examples

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic if the AIP SSM card fails for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM card fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
```

```
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

Related Commands

Command	Description
allocate-ips	Assigns a virtual sensor to a security context.
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current **policy-map** configurations.

ipsec-udp

To enable IPSec over UDP, use the **ipsec-udp enable** command in group-policy configuration mode. To disable IPSec over UDP, use the **ipsec-udp disable** command. To remove the IPSec over UDP attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for IPSec over UDP from another group policy.

IPSec over UDP, sometimes called IPSec through NAT, lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ipsec-udp {enable | disable}

no ipsec-udp

Syntax Description

disable	Disables IPSec over UDP.
enable	Enables IPSec over UDP.

Defaults

IPSec over UDP is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To use IPSec over UDP, you must also configure the **ipsec-udp-port** command.

The Cisco VPN Client must also be configured to use IPSec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPSec over UDP.

IPSec over UDP is proprietary, it applies only to remote-access connections, and it requires mode configuration, means the security appliance exchanges configuration parameters with the client while negotiating SAs.

Using IPSec over UDP may slightly degrade system performance.

Examples

The following example shows how to set IPSec over UDP for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

Related Commands

Command	Description
ipsec-udp-port	Specifies the port on which the security appliance listens for UDP traffic.

ipsec-udp-port

To set a UDP port number for IPSec over UDP, use the **ipsec-udp-port** command in group-policy configuration mode. To disable the UDP port, use the **no** form of this command. This enables inheritance of a value for the IPSec over UDP port from another group policy.

In IPSec negotiations. the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic.

ipsec-udp-port *port*

no ipsec-udp-port

Syntax Description

port	Identifies the UDP port number using an integer in the range 4001 through 49151.

Defaults

The default port is 10000.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can configure multiple group policies with this feature enabled, and each group policy can use a different port number.

Examples

The following example shows how to set an IPSec UDP port to port 4025 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

Command	Description
ipsec-udp	Lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ip verify reverse-path

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. To disable this feature, use the **no** form of this command. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

Syntax Description

interface_name	The interface on which you want to enable Unicast RPF.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Normally, the security appliance only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the security appliance to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the security appliance can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the security appliance uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.

- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

Examples

The following example enables Unicast RPF on the outside interface:

```
hostname(config)# ip verify reverse-path interface outside
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

ipv6 access-list

To configure an IPv6 access list, use the **ipv6 access-list** command in global configuration mode. To remove an ACE, use the **no** form of this command. Access lists define the traffic that the security appliance allows to pass through or blocks.

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

Syntax Description

any	An abbreviation for the IPv6 prefix ::/0, indicating any IPv6 address.
default	(Optional) Specifies that a syslog message 106100 is generated for the ACE.
deny	Denies access if the conditions are matched.
destination-ipv6-address	The IPv6 address of the host receiving the traffic.
destination-ipv6-prefix	The IPv6 network address where the traffic is destined.
disable	(Optional) Disables syslog messaging.
host	Indicates that the address refers to a specific host.
icmp6	Specifies that the access rule applies to ICMPv6 traffic passing through the security appliance.

icmp_type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect Omitting the *icmp_type* argument indicates all ICMP types.
icmp_type_obj_grp_id	(Optional) Specifies the object group ICMP type ID.
id	Name or number of an access list.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds. The default interval is 300 seconds. This value is also used as the timeout value for deleting an inactive flow.
level	(Optional) Specifies the syslog level for message 106100; valid values are from 0 to 7. The default level is 6 (informational).
line *line-num*	(Optional) The line number where the access rule is being inserted into the list. If you do not specify a line number, the ACE is added to the end of the access list.
log	(Optional) Specifies the logging action for the ACE. If you do not specify the **log** keyword or you specify the **log default** keyword, then message 106023 is generated when a packet is denied by the ACE. If you sepcify the log keyword alone or with a level or interval, then message 106100 is generated when a packet is denied by the ACE. Packets that are denied by the implicit deny at the end of an access list are not logged. You must explicitly deny packets with an ACE to enable logging.
network_obj_grp_id	Existing network object group identification.
object-group	(Optional) Specifies an object group.

operator	(Optional) Specifies the operand to compare the source IP address to the destination IP address. The *operator* compares the source IP address or destination IP address ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **ipv6 access-list** command without an operator and port to indicate all ports by default.
permit	Permits access if the conditions are matched.
port	(Optional) Specifies the port that you permit or deny access. When entering the *port* argument, you can specify the port by either a number in the range of 0 to 65535 or a using literal name if the *protocol* is **tcp** or **udp**. Permitted TCP literal names are **aol, bgp**, **chargen**, **cifc**, **citrix-ica**, **cmd**, **ctiqbe**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **https**, **ident**, **irc**, **kerberos**, **klogin**, **kshell**, **ldap**, **ldaps**, **login**, **lotusnotes**, **lpd**, **netbios-ssn**, **nntp**, **pop2**, **pop3**, **pptp**, **rsh**, **rtsp**, **smtp**, **sqlnet**, **ssh**, **sunrpc, tacacs, talk, telnet, uucp, whois, and www**. Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **cifs**, **discard**, **dnsix**, **domain**, **echo**, **http**, **isakmp**, **kerberos**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **ntp**, **pcanywhere-status**, **pim-auto-rp**, **radius**, **radius-acct**, **rip**, **secureid-udp**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, **www**, and **xdmcp**.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
protocol	Name or number of an IP protocol; valid values are **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number.
protocol_obj_grp_id	Existing protocol object group identification.
service_obj_grp_id	(Optional) Specifies the object group.
source-ipv6-address	The IPv6 address of the host sending the traffic.
source-ipv6-prefix	The IPv6 network address of the where the network traffic originated.

Defaults

When the **log** keyword is specified, the default level for syslog message 106100 is 6 (informational).

The default logging interval is 300 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command allows you to specify if an IPv6 address is permitted or denied access to a port or protocol. Each command is called an ACE. One or more ACEs with the same access list name are referred to as an access list. Apply an access list to an interface using the **access-group** command.

The security appliance denies all packets from an outside interface to an inside interface unless you specifically permit access using an access list. All packets are allowed by default from an inside interface to an outside interface unless you specifically deny access.

The **ipv6 access-list** command is similar to the **access-list** command, except that it is IPv6-specific. For additional information about access lists, refer to the **access-list extended** command.

The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the security appliance.To configure the ICMPv6 traffic that is allowed to originate and terminate at a specific interface, use the **ipv6 icmp** command.

Refer to the **object-group** command for information on how to configure object groups.

Examples

The following example will allow any host using TCP to access the 3001:1::203:A0FF:FED6:162D server:

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
```

The following example uses **eq** and a port to deny access to just FTP:

```
hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp
hostname(config)# access-group acl_out in interface inside
```

The following example uses **lt** to permit access to all ports less than port 2025, which permits access to the well-known ports (1 to 1024):

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host 3001:1::203:A0FF:FED6:162D
lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

Related Commands

Command	Description
access-group	Assigns an access list to an interface.
ipv6 icmp	Configures access rules for ICMP messages that terminate at an interface of the security appliance.
object-group	Creates an object group (addresses, ICMP types, and services).

ipv6 access-list webtype

To create an ipv6 access list that you can add to a configuration that supports filtering for clientless SSL VPN, use the **access-list webtype** command in global configuration mode. To remove the access list, use the **no** form of this command with the entire syntax string as it appears in the configuration.

ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

no ipv6 access-list *id* **webtype** {**deny** | **permit**} **url** [**url_string** | **any**]

Syntax Description

id	Name or number of an access list.
any	Specifies access to anyone.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are met.
url	Specifies that a URL be used for filtering.
url_string	(Optional) Specifies the URL to be filtered.

Defaults

The defaults are as follows:

- The adaptive security appliance denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates system log message 106023 for denied packets—deny packets must be present to log denied packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

You can use the following wildcard characters to define more than one wildcard in the Webtype access list entry:

- Enter an asterisk "*" to match no characters or any number of characters.
- Enter a question mark "?" to match any one character exactly.
- Enter square brackets "[]" to create a range operator that matches any one character in a range.

Examples

The examples in this section show how to use wildcards in IPv6 Webtype access lists.

- The following example matches URLs such as http://www.cisco.com/ and http://wwz.caco.com/:

```
ipv6 access-list test webtype permit url http://ww?.c*co*/
```

- The following example matches URLs such as http://www.cisco.com and ftp://wwz.carrier.com:

```
ipv6 access-list test webtype permit url *://ww?.c*co*/
```

- The following example matches URLs such as http://www.cisco.com:80 and https://www.cisco.com:81:

```
ipv6 access-list test webtype permit url *://ww?.c*co*:8[01]/
```

  The range operator "[]" in the preceding example specifies that either character 0 or 1 can occur.

- The following example matches URLs such as http://www.google.com and http://www.boogie.com:

```
ipv6 access-list test webtype permit url http://www.[a-z]oo?*/
```

  The range operator "[]" in the preceding example specifies that any character in the range from a to z can occur.

- The following example matches URLs such as http://www.cisco.com/anything/crazy/url/ddtscgiz:

```
ipv6 access-list test webtype permit url htt*://*/*cgi?*
```

Note To match any http URL, you must enter http://*/* instead of the former method of entering http://*.

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the adaptive security appliance.
clear access-group	Clears an access list counter.
show running-config access-list	Displays the access-list configuration running on the adaptive security appliance.

ipv6 address

To enable IPv6 and configure the IPv6 addresses on an interface, use the **ipv6 address** command in interface configuration mode. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

no ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

Syntax Description

autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface.
eui-64	(Optional) Specifies an interface ID in the low order 64 bits of the IPv6 address.
ipv6-address	The IPv6 link-local address assigned to the interface.
ipv6-prefix	The IPv6 network address assigned to the interface.
link-local	Specifies that the address is a link-local address.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).

Defaults

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring an IPv6 address on an interface enables IPv6 on that interface; you do not need to use the **ipv6 enable** command after specifying an IPv6 address.

The **ipv6 address autoconfig** command is used to enable automatic configuration of IPv6 addresses on an interface using stateless autoconfiguration. The addresses are configured based on the prefixes received in Router Advertisement messages. If a link-local address has not been configured, then one is automatically generated for this interface. An error message is displayed if another host is using the link-local address.

The **ipv6 address eui-64** command is used to configure an IPv6 address for an interface. If the optional **eui-64** is specified, the EUI-64 interface ID will be used in the low order 64 bits of the address. If the value specified for the *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID. An error message will be displayed if another host is using the specified address.

The Modified EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64 bit interface ID of 02E0:B6FF:FE01:3B7A.

The **ipv6 address link-local** command is used to configure an IPv6 link-local address for an interface. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface. The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in Modified EUI-64 format. An interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error message will be displayed if another host is using the specified address.

Examples

The following example assigns 3FFE:C00:0:1::576/64 as the global address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

The following example assigns an IPv6 address automatically for the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

The following example assigns IPv6 address 3FFE:C00:0:1::/64 to the selected interface and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

Related Commands

Command	Description
debug ipv6 interface	Displays debug information for IPv6 interfaces.
show ipv6 interface	Displays the status of interfaces configured for IPv6.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing.

The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address for an interface and enables IPv6 processing on the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 enforce-eui64

To enforce the use of Modified EUI-64 format interface identifiers in IPv6 addresses on a local link, use the **ipv6 enforce-eui64** command in global configuration mode. To disable Modified EUI-64 address format enforcement, use the **no** form of this command.

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

Syntax Description

if_name	Specifies the name of the interface, as designated by the **nameif** command, for which you are enabling Modified EUI-64 address format enforcement.

Defaults

Modified EUI-64 format enforcement is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When this command is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link. Packets received from hosts behind a router will fail the address format verification, and be dropped, because their source MAC address will be the router MAC address and not the host MAC address.

The Modified EUI-64 format interface identifier is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64 bit interface ID of 02E0:B6FF:FE01:3B7A.

Examples

The following example enables Modified EUI-64 format enforcement for IPv6 addresses received on the inside interface:

```
hostname(config)# ipv6 enforce-eui64 inside
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address on an interface.
ipv6 enable	Enables IPv6 on an interface.

ipv6 icmp

To configure ICMP access rules for an interface, use the **ipv6 icmp** command in global configuration mode. To remove an ICMP access rule, use the **no** form of this command.

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

Syntax Description

any	Keyword specifying any IPv6 address. An abbreviation for the IPv6 prefix ::/0.
deny	Prevents the specified ICMP traffic on the selected interface.
host	Indicates that the address refers to a specific host.
icmp-type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	The name of the interface, as designated by the **nameif** command, the access rule applies to.
ipv6-address	The IPv6 address of the host sending ICMPv6 messages to the interface.
ipv6-prefix	The IPv6 network that is sending ICMPv6 messages to the interface.
permit	Allows the specified ICMP traffic on the selected interface.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Defaults

If no ICMP access rules are defined, all ICMP traffic is permitted.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

If there are no ICMP rules defined for an interface, all IPv6 ICMP traffic is permitted.

If there are ICMP rules defined for an interface, then the rules are processed in order on a first-match basis followed by an implicit deny all rule. For example, if the first matched rule is a permit rule, the ICMP packet is processed. If the first matched rule is a deny rule, or if the ICMP packet did not match any rule on that interface, then the security appliance discards the ICMP packet and generates a syslog message.

For this reason, the order that you enter the ICMP rules is important. If you enter a rule denying all ICMP traffic from a specific network, and then follow it with a rule permitting ICMP traffic from a particular host on that network, the host rule will never be processed. The ICMP traffic is blocked by the network rule. However, if you enter the host rule first, followed by the network rule, the host ICMP traffic will be allowed, while all other ICMP traffic from that network is blocked.

The **ipv6 icmp** command configures access rules for ICMP traffic that terminates at the security appliance interfaces. To configure access rules for pass-through ICMP traffic, refer to the **ipv6 access-list** command.

Examples

The following example denies all ping requests and permits all Packet Too Big messages (to support Path MTU Discovery) at the outside interface:

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

ipv6 local pool

To configure an IPv6 address pool from which to allocate addresses to remote clients, use the **ipv6 local pool** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command.

ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

no ipv6 local pool *pool_name ipv6_address/prefix_length number_of_addresses*

Syntax Description

pool_name	Specifies the name to assign to this IPv6 address pool.
ipv6_address	Specifies the IPv6 address pool being configured. The format is x:x:x::
number_of_addresses	Range: 1-16384
prefix_length	Range: 0-128

Defaults

By default, the IPv6 local address pool is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To assign IPv6 local pools, use either the **ipv6-local-pool** command in the tunnel-group or the **ipv6-address-pools** (note the "s" on this one) command in the group policy. The ipv6-address-pools setting in the group policy overrides the ipv6-address-pool setting in the tunnel group.

Examples

The following example, entered in config-general configuration mode, configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients:

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
hostname(config)#
```

Related Commands

Command	Description
ipv6-address-pool	Associates IPv6 address pools with a VPN tunnel group policy.
ipv6-address-pools	Associates IPv6 address pools with a VPN group policy.
clear configure ipv6 local pool	Clears all configured IPv6 local pools.
show running-config ipv6	Shows the configuration for IPv6.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection, use the **ipv6 nd dad attempts** command in interface configuration mode. To return to the default number of duplicate address detection messages sent, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

Syntax Description

value	A number from 0 to 600. Entering 0 disables duplicate address detection on the specified interface. Entering 1 configures a single transmission without follow-up transmissions. The default value is 1 message.

Defaults

The default number of attempts is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. The frequency at which the neighbor solicitation messages are sent is configured using the **ipv6 nd ns-interval** command.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state.

Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up. An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

Note While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Examples

The following example configures 5 consecutive neighbor solicitation messages to be sent when duplicate address detection is being performed on the tentative unicast IPv6 address of the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

Syntax Description

value	The interval between IPv6 neighbor solicitation transmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds.

Defaults

1000 milliseconds between neighbor solicitation transmissions.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for Gigabitethernet 0/0:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

Syntax Description

at *valid-date preferred-date*	The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire*.
default	Default values are used.
infinite	(Optional) The valid lifetime does not expire.
ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no-advertise	(Optional) Indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is not used for on-link determination.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 604800 (7 days).
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
valid-lifetime	The amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with **infinite**. The default is 2592000 (30 days).

Defaults

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is "on" (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is "on" (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds, in router advertisements sent out on the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	(Optional) indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is seconds.
value	The interval between IPv6 router advertisement transmissions. Valid values range from 3 to 1800 seconds, or from 500 to 1800000 milliseconds if the **msec** keyword is provided. The default is 200 seconds.

Defaults

200 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the security appliance is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

To configure the "router lifetime" value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

Syntax Description

seconds	The validity of the security appliance as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the security appliance should not be considered a default router on the selected interface.

Defaults

1800 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The "router lifetime" value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the security appliance as a default router on this interface.

Setting the value to a non-zero value to indicates that the security appliance should be considered a default router on this interface. The no-zero value for the "router lifetime" value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the security appliance should not be considered a default router on this interface.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

Syntax Description

value	The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default value is 0. When 0 is used for the *value*, the reachable time is sent as undetermined. It is up to the receiving devices to set and track the reachable time value.

Defaults

0 milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

To see the reachable time used by the security appliance, including the actual value when this comamnd is set to 0, use the **show ipv6 interface** command to display information about the IPv6 interface, including the ND reachable time being used.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Defaults

Router advertisements are automatically sent on LAN interfaces if IPv6 unicast routing is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static entry from the neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

Syntax Description

if_name	The internal or external interface name designated by the **nameif** command.
ipv6_address	The IPv6 address that corresponds to the local data-link address.
mac_address	The local data-line (hardware MAC) address.

Defaults

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the **copy** command is used to store the configuration.

Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example adds a static entry for the an inside host with an IPv6 address of 3001:1::45A and a MAC address of 0002.7D1A.9472 to the neighbor discovery cache:

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

ipv6 route

To add an IPv6 route to the IPv6 routing table, use the **ipv6 route** command in global configuration mode. To remove an IPv6 default route, use the **no** form of this command.

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

Syntax Description

administrative-distance	(Optional) The administrative distance of the route. The default value is 1, which gives static routes precedence over any other type of routes except connected routes.
if_name	The name of the interface the route is being configured for.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network.
ipv6-prefix	The IPv6 network that is the destination of the static route. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
tunneled	(Optional) Specifies route as the default tunnel gateway for VPN traffic.

Defaults

By default, the *administrative-distance* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **show ipv6 route** command to view the contents of the IPv6 routing table.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the security appliance that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled** option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route. Doing so causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

Examples

The following example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 with an administrative distance of 110:

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

Command	Description
debug ipv6 route	Displays debug messages for IPv6 routing table updates and route cache updates.
show ipv6 route	Displays the current contents of the IPv6 routing table.

ipv6-address-pool (tunnel-group general attributes mode)

To specify a list of IPv6 address pools for allocating addresses to remote clients, use the **ipv6-address-pool** command in tunnel-group general-attributes configuration mode. To eliminate IPv6 address pools, use the **no** form of this command.

ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pool [(*interface_name*)] *ipv6_address_pool1* [*...ipv6_address_pool6*]

Syntax Description

ipv6_address_pool	Specifies the name of the address pool configured with the **ipv6 local pool** command. You can specify up to 6 local address pools.
interface_name	(Optional) Specifies the interface to be used for the address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

The IPv6 address-pool settings in the group-policy **ipv6-address-pools** command override the IPv6 address pool settings in the tunnel group **ipv6-address-pool** command.

The order in which you specify the pools is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

Examples

The following example entered in config-tunnel-general configuration mode, specifies a list of IPv6 address pools for allocating addresses to remote clients for an IPSec remote-access tunnel group test:

```
hostname(config)# tunnel-group test type remote-access
hostname(config)# tunnel-group test general-attributes
hostname(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
ipv6addrpool3
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
ipv6-address-pools	Configures the IPv6 address pools settings for the group policy; these settings override those for the tunnel-group.
ipv6 local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group	Configures a tunnel group.

ipv6-address-pools

To specify a list of up to six IPv6 address pools from which to allocate addresses to remote clients, use the **ipv6-address-pools** command in group-policy attributes configuration mode. To remove the attribute from the group policy and enable inheritance from other sources of group policy, use the **no** form of this command.

ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

no ipv6-address-pools value *ipv6_address_pool1* [*...ipv6_address_pool6*]

ipv6-address-pools none

no ipv6-address-pools none

Syntax Description

ipv6_address_pool	Specifies the names of the up to six IPv6 address pools configured with the **ipv6 local pool** command. Use spaces to separate the IPv6address pool names.
none	Specifies that no IPv6 address pools are configured and disables inheritance from other sources of group policy.
value	Specifies a list of up to six IPv6 address pools from which to assign addresses.

Defaults

By default, the IPv6 address pools attribute is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To configure IPv6 address pools, use the **ipv6 local pool** command.

The order in which you specify the pools in the **ipv6-address-pools** command is significant. The security appliance allocates addresses from these pools in the order in which the pools appear in this command.

The command **ipv6-address-pools none** disables this attribute from being inherited from other sources of policy, such as the DefaultGrpPolicy. The command **no ipv6-address-pools none** removes the **ipv6-address-pools none** command from the configuration, restoring the default value, which is to allow inheritance.

Examples

The following example, entered in config-general configuration mode, configures an IPv6 address pool named firstipv6pool for use in allocating addresses to remote clients, then associates that pool with GroupPolicy1:

```
hostname(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# ipv6-address-pools value firstipv6pool
hostname(config-group-policy)#
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool to be used for VPN group policies.
clear configure group-policy	Clears all configured group policies.
show running-config group-policy	Shows the configuration for all group-policies or for a particular group-policy.

ipv6-vpn-filter

To specify the name of the ACL to use for VPN connections, use the **ipv6-vpn-filter** command in group policy or username mode. To remove the ACL, including a null value created by issuing the **ipv6-vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **ipv6-vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **ipv6-vpn-filter** command to apply those ACLs.

ipv6-vpn-filter {**value** *IPV6-ACL-NAME* | **none**}

no ipv6-vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *IPV6-ACL-NAME*	Provides the name of the previously configured access list.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Clientless SSL VPN does not use the ACL defined in the **ipv6-vpn-filter** command.

Examples

The following example shows how to set a filter that invokes an access list named ipv6_acl_vpn for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipv6-vpn-filter value ipv6_acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.

isakmp am-disable

To disable inbound aggressive mode connections, use the **isakmp am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

isakmp am-disable

no isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command was deprecated. The **crypto isakmp am-disable** command replaces it.

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
hostname(config)# isakmp am-disable
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp disconnect-notify

To enable disconnect notification to peers, use the **isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

isakmp disconnect-notify

no isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command was deprecated. The **crypto isakmp disconnect-notify** command replaces it.

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance, use the **isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

isakmp enable *interface-name*

no isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp enable** command replaces it.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
hostname(config)# no isakmp enable inside
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp identity

To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully-qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Defaults

The default ISAKMP identity is **isakmp identity hostname**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp identity** command replaces it.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPSec peer, depending on connection type:

```
hostname(config)# isakmp identity auto
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp ikev1-user-authentication

To configure hybrid authentication during IKE, use the **isakmp ikev1-user-authentication** command in tunnel-group ipsec-attributes configuration mode. To disable hybrid authentication, use the **no** form of this command.

isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

Syntax Description

hybrid	Specifies hybrid XAUTH authentication during IKE.
interface	(Optional) Specifies the interface on which the user authentication method is configured.
none	Disables user authentication during IKE.
xauth	Specifies XAUTH, also called extended user authentication.

Defaults

The default authentication method is XAUTH or extended user authentication. The default *interface* is all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You use this command when you need to use digital certificates for security appliance authentication and a different, legacy method for remote VPN user authentication, such as RADIUS, TACACS+ or SecurID. This command breaks phase 1 of IKE down into the following two steps, together called hybrid authentication:

1. The security appliance authenticates to the remote VPN user with standard public key techniques. This establishes an IKE security association that is unidirectionally authenticated.
2. An XAUTH exchange then authenticates the remote VPN user. This extended authentication can use one of the supported legacy authentication methods.

Note Before the authentication type can be set to hybrid, you must configure the authentication server, create a preshared key, and configure a trustpoint.

When you omit the optional **interface** parameter, the command applies to all the interfaces and serves as a back-up when the per-interface command is not specified. When there are two **isakmp ikev1-user-authentication** commands specified for a tunnel group, and one uses the **interface** parameter and one does not, the one specifying the interface takes precedence for that particular interface.

Examples

The following example commands enable hybrid XAUTH on the inside interface for a tunnel group called example-group:

```
hostname(config)# tunnel-group example-group type ipsec-ra
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
aaa-server	Defines a AAA server.
pre-shared-key	Creates a preshared key for supporting IKE connections.
tunnel-group	Creates and manages the database of connection specific records for IPSec, L2TP/IPSec and WebVPN connections.

isakmp ipsec-over-tcp

To enable IPSec over TCP, use the **isakmp ipsec-over-tcp** command in global configuration mode. To disable IPSec over TCP, use the **no** form of this command.

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPSec over TCP connections. You can list up to 10 ports. Port numbers can be in the range 1-65535. The default port number is 10000.

Defaults

The default value is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command was deprecated. The **crypto isakmp ipsec-over-tcp** command replaces it.

Examples

This example, entered in global configuration mode, enables IPSec over TCP on port 45:

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp keepalive

To configure IKE DPD, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

isakmp keepalive [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

no isakmp keepalive disable

Syntax Description

disable	Disables IKE keepalive processing, which is enabled by default.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10 seconds for a LAN-to-LAN group, and 300 second for a remote access group.

Defaults

The default for a remote access group is a threshold of 300 seconds and a retry of 2 seconds.

For a LAN-to-LAN group, the default is a threshold of 10 seconds and a retry of 2 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to IPSec remote-access and IPSec LAN-to-LAN tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, configures IKE DPD, establishes a threshold of 15, and specifies a retry interval of 10 for the IPSec LAN-to-LAN tunnel group with the IP address 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

isakmp nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **isakmp enable** command) in global configuration mode and then use the **isakmp nat-traversal** command. If you have enabled NAT traversal, you can disable it with the **no** form of this command.

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Defaults

By default, NAT traversal (**isakmp nat-traversal**) is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp nat-traversal** command replaces it.

Usage Guidelines

Network Address Translation (NAT), including Port Address Translation (PAT), is used in many networks where IPSec is also used, but there are a number of incompatibilities that prevent IPSec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The security appliance supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html, and NAT traversal is supported for both dynamic and static crypto maps.

This command enables NAT-T globally on the security appliance. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then enables NAT traversal with an interval of 30 seconds:

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy authentication

To specify an authentication method within an IKE policy, use the **isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To remove the ISAKMP authentication method, use the related **clear configure** command.

isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

Syntax Description

crack	Specifies IKE Challenge/Response for Authenticated Cryptographic Keys (CRACK) as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This basically means you can prove to a third party whether you had an IKE negotiation with the peer.

Defaults

The default ISAKMP policy authentication is **pre-share**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting. DSA-Sig was added in 7.0.

Usage Guidelines

If you specify RSA signatures, you must configure the security appliance and its peer to obtain certificates from a certification authority (CA). If you specify preshared keys, you must separately configure these preshared keys within the security appliance and its peer.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy authentication** command. This example sets the authentication method of RSA Signatures to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is **des,** use the **no** form of this command.

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

Syntax Description

3des	Specifies that the Triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default ISAKMP policy encryption is **3des**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp policy encryption** command replaces it.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
hostname(config)# isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 encryption 3des
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

isakmp policy *priority* **group** {**1** | **2** | **5**}

no isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default is group 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting. Group 7 was added.
7.2(1)	This command was deprecated. The **crypto isakmp policy group** command replaces it.
8.0(4)	The **group 7** command option was **deprecated**. Attempts to configure group 7 will generate an error message and use group 5 instead.

Usage Guidelines

There are three group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), and 1536-bit (DH Group 5). The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires **isakmp policy** to have DH **group 2** configured. (If you have DH **group 1** configured, the Cisco VPN Client cannot connect.)

AES support is available on security appliances licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) **group 5** instead of **group 1** or **group 2**. This is done with the **isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy group** command. This example sets group 2, the 1024-bit Diffie Hellman, to use for the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 group 2
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

isakmp policy *priority* **hash** {**md5** | **sha**}

no isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies that SHA-1 (HMAC variant) as the hash algorithm be used in the IKE policy.

Defaults

The default hash algorithm is SHA-1 (HMAC variant).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp policy hash** command replaces it.

Usage Guidelines

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy hash** command. This example specifies that the MD5 hash algorithm be used within the IKE policy, with the priority number of 40.

```
hostname(config)# isakmp policy 40 hash md5
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **isakmp policy lifetime** command in global configuration mode. Use the **no** form of this command to reset the security association lifetime to the default value of 86,400 seconds (one day).

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for infinite lifetime.

Defaults

The default value is 86,400 seconds (one day).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was deprecated. The **crypto isakmp policy lifetime** command replaces it.

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPSec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the security appliance sets up future IPSec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default, but y ou can specify an infinite lifetime if the peer does not propose a lifetime.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.
The following example, entered in global configuration mode, shows use of the **isakmp policy lifetime** command. This example sets the lifetime of the IKE security association to 50,400 seconds (14 hours) within the IKE policy with the priority number of 40.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
hostname(config)# isakmp policy 40 lifetime 0
```

Related Commands

clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the security appliance, use the **isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the security appliance, use the **no** form of this command.

isakmp reload-wait

no isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
7.2(1)	This command was deprecated. The **crypto isakmp reload-wait** command replaces it.

Examples

The following example, entered in global configuration mode, tells the security appliance to wait until all active sessions have terminated before rebooting.

```
hostname(config)# isakmp reload-wait
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

issuer

To specify the security device that is sending assertions to a SAML-type SSO server, use the **issuer** command in webvpn-sso-saml configuration mode for that specific SAML type. To remove the issuer name, use the **no** form of this command.

issuer *identifier*

no issuer [*identifier*]

Syntax Description

identifier	Specifies a security device name, usually the hostname of the device. An identifier must be less than 65 alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn-sso-saml configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

Examples

The following example specifies the issuer name for a security device named asa1.mycompany.com:

```
hostname(config-webvpn)# sso server myhostname type saml-v1.1-post
hostname(config-webvpn-sso-saml# issuer asa1.example.com
hostname(config-webvpn-sso-saml#
```

Related Commands

Command	Description
assertion-consumer-url	Specifies the URL that the security device uses to contact the SAML-type SSO server assertion consumer service.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion.

issuer-name

To specify the issuer-name DN of all issued certificates, use the **issuer-name** command in local Certificate Authority (CA) server configuration mode. To remove the subject-DN from the certificate authority certificate, use the **no** form of this command.

issuer-name *DN-string*

no issuer-name [*DN-string*]

Syntax Description

DN-string	Specifies the distinguished name of the certificate, which is also the subject-name DN of the self-signed CA certificate. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. An issuer-name must be less than 500 alphanumeric characters.

Defaults

The default issuer-name is cn=*hostame.domain-name*, such as cn=asa.example.com.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
7.3(1)	This command was introduced.
8.0(2)	Support for quotation marks added to retain commas in *DN-string* values.

Usage Guidelines

This command specifies the issuer name that appears on any certificate created by this local CA server. Use this optional command if you want the issuer name to be different from the default CA name.

Note This issuer name configuration cannot be changed once you enable the CA server and generate the certificate by issuing the **no shutdown** command.

Examples

The following example configures certificate authentication:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco
systems, inc."
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
keysize	Specifies the size of the public and private keys generated at certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate and issued certificates.
show crypto ca server	Displays the characteristics of the local CA.
show crypto ca server cert-db	Displays local CA server certificates.

CHAPTER 17

java-trustpoint through kill Commands

java-trustpoint

To configure the WebVPN Java object signing facility to use a PKCS12 certificate and keying material from a specified trustpoint location, use the **java-trustpoint** command in Webvpn configuration mode.

To remove a trustpoint for Java object signing, use the **no** form of this command.

java-trustpoint *trustpoint*

no java-trustpoint

Syntax Description

trustpoint	Specifies the trustpoint location configured by the **crypto ca import** command.

Defaults

By default, a trustpoint for Java object signing is set to none.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(2)	This command was introduced.

Usage Guidelines

A trustpoint is a representation of a certificate authority (CA) or identity key pair. For the java-trustpoint command, the given trustpoint must contain the X.509 certificate of the application signing entity, the RSA private key corresponding to that certificate, and a certificate authority chain extending up to a root CA. This is typically achieved by using the **crypto ca import** command to import a PKCS12 formatted bundle. You can obtain a PKCS12 bundle from a trusted CA authority or you can manually create one from an existing X.509 certificate and an RSA private key using open source tools such as openssl.

Examples

This following example first configures a new trustpoint and then configures it for WebVPN Java object signing. The following command creates a new trustpoint called my mytrustpoint:

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)#
```

The following example configures the new trustpoint for signing WebVPN Java objects:

```
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

Related Commands

Command	Description
crypto ca import	Imports the certificate and key pair for a trustpoint using PKCS12 data.

join-failover-group

To assign a context to a failover group, use the **join-failover-group** command in context configuration mode. To restore the default setting, use the **no** form of this command.

join-failover-group *group_num*

no join-failover-group *group_num*

Syntax Description

group_num	Specifies the failover group number.

Defaults

Failover group 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The admin context is always assigned to failover group 1. You can use the **show context detail** command to display the failover group and context association.

Before you can assign a context to a failover group, you must create the failover group with the **failover group** command in the system context. Enter this command on the unit where the context is in the active state. By default, unassigned contexts are members of failover group 1, so if the context had not been previously assigned to a failover group, you should enter this command on the unit that has failover group 1 in the active state.

You must remove all contexts from a failover group, using the **no join-failover-group** command, before you can remove a failover group from the system.

Examples

The following example assigns a context named ctx1 to failover group 2:

```
hostname(config)# context ctx1
hostname(config-context)# join-failover-group 2
hostname(config-context)# exit
```

Related Commands

Command	Description
context	Enters context configuration mode for the specified context.
failover group	Defines a failover group for Active/Active failover.
show context detail	Displays context detail information, including name, class, interfaces, failover group association, and configuration file URL.

keepout

To present a keepout webpage rather than a login page for new user sessions when the security appliance undergoes a maintenance or troubleshooting period, use the **keepout** command in webvpn configuration mode. To remove a previously set keepout page use the **no** version of the command.

keepout

no keepout *string*

Syntax Description

string	An alphanumeric string in double quotation marks.

Defaults

No keepout page.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the keepout command to communicate unavailability of the security appliance.

Examples

The following example shows how to configure a keepout page:

```
hostname(config)# webvpn
hostname(config-webvpn)# keepout "The system is unavailable until 7:00 a.m. EST."
hostname(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn configuration mode, which lets you configure attributes for clientless SSLVPN connections.

kerberos-realm

To specify the realm name for this Kerberos server, use the **kerberos-realm** command in aaa-server host configuration mode. To remove the realm name, use the **no** form of this command:

kerberos-realm *string*

no kerberos-realm

Syntax Description

string	A case-sensitive, alphanumeric string, up to 64 characters long. Spaces are not permitted in the string. **Note** Kerberos realm names use numbers and upper-case letters only. Although the security appliance accepts lower-case letters in the *string* argument, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Introduced in this release.

Usage Guidelines

This command is valid only for Kerberos servers.

The value of the *string* argument should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Windows 2000 Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

The *string* argument must use numbers and upper-case letters only. The **kerberos-realm** command is case sensitive and the security appliance does not translate lower-case letters to upper-case letters.

Examples

The following sequence shows the **kerberos-realm** command to set the kerberos realm to "EXAMPLE.COM" in the context of configuring a AAA server host:

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration submode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

key

To specify the server secret value used to authenticate the NAS to the AAA server, use the **key** command in aaa-server host configuration mode. The Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove the key, use the **no** form of this command.

key *key*

no key

Syntax Description

key	An alphanumeric keyword, up to 127 characters long.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The *key* value is a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. Any characters entered past 127 are ignored. The key is used between the client and the server for encrypting data between them. The key must be the same on both the client and server systems.The key cannot contain spaces, but other special characters are allowed. The key (server secret) value authenticates the security appliance to the AAA server.

This command is valid only for RADIUS and TACACS+ servers.

The **key** parameter of the **aaa-server** command in earlier PIX firewall versions is automatically converted to the equivalent **key** command.

Examples

The following example configures a TACACS+ AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the key as “myexclusivemumblekey”.

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server configuration.

keypair

To specify the key pair whose public key is to be certified, use the **keypair** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

keypair *name*

no keypair

Syntax Description

name	Specify the name of the key pair.

Defaults

The default setting is not to include the key pair.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and specifies a key pair to be certified for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
crypto key generate dsa	Generates DSA keys.
crypto key generate rsa	Generates RSA keys.
default enrollment	Returns enrollment parameters to their defaults.

keysize

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server at user certificate enrollment, use the **keysize** command in CA server configuration mode. To reset the keysize to the default length of 1024 bits, use the **no** form of this command.

keysize {**512** | **768** | **1024** | **2048**}

no keysize

Syntax Description

512	Specifies a size of 512 bits for the public and private keys generated at certificate enrollment.
768	Specifies a size of 768 bits for the public and private keys generated at certificate enrollment.
1024	Specifies a size of 1024 bits for the public and private keys generated at certificate enrollment.
2048	Specifies a size of 2048 bits for the public and private keys generated at certificate enrollment.

Defaults

By default, the each key in the key pair is 1024 bits long.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies a key size of 2048 bits for all public and private key pairs generated for users by the local CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize 2048
hostname(config-ca-server)#
```

The following example resets the key size to the default length of 1024 bits for all public and private key pairs generated for users by the local CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no keysize
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

keysize server

To specify the size of the public and private keys generated by the local Certificate Authority (CA) server for configure the size of the CAs own keypair, use the **keysize server** command in CA server configuration mode. To reset the keysize to the default length of 1024 bits, use the no form of this command.

keysize server{**512** | **768** | **1024** | **2048**}

no keysize server

Syntax Description

512	Specifies a size of 512 bits for the public and private keys generated at certificate enrollment.
768	Specifies a size of 768 bits for the public and private keys generated at certificate enrollment.
1024	Specifies a size of 1024 bits for the public and private keys generated at certificate enrollment.
2048	Specifies a size of 2048 bits for the public and private keys generated at certificate enrollment.

Defaults

By default, the each key in the key pair is 1024 bits long.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies a key size of 2048 bits for the CAs own certificate:

```
hostname(config)# crypto ca server
hostname(config-ca-server))# keysize server 2048
hostname(config-ca-server)#
```

The following example resets the key size to the default length of 1024 bits for the CAs own certificate:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no keysize server
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the key pair size for the user certificate.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

kill

To terminate a Telnet session, use the **kill** command in privileged EXEC mode.

kill *telnet_id*

Syntax Description

telnet_id	Specifies the Telnet session ID.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **kill** command lets you terminate a Telnet session. Use the **who** command to see the Telnet session ID. When you kill a Telnet session, the security appliance lets any active commands terminate and then drops the connection without warning.

Examples

The following example shows how to terminate a Telnet session with the ID "2". First, the **who** command is entered to display the list of active Telnet sessions. Then the **kill 2** command is entered to terminate the Telnet session with the ID "2".

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

Related Commands

Command	Description
telnet	Configures Telnet access to the security appliance.
who	Displays a list of active Telnet sessions.

CHAPTER 18

l2tp tunnel hello through log-adj-changes Commands

l2tp tunnel hello

To specify the interval between hello messages on L2TP over IPSec connections, use the **l2tp tunnel hello** command in global configuration mode. To reset the interval to the default, use the **no** form of the command:

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

Syntax Description

interval	Interval between hello messages in seconds. The Default is 60 seconds. The range is 10 to 300 seconds.

Defaults

The default is 60 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **l2tp tunnel hello** command enables the security appliance to detect problems with the physical layer of the L2TP connection. The default is 60 secs. If you configure it to a lower value, connections that are experiencing problems are disconnected earlier.

Examples

The following example configures the interval between hello messages to 30 seconds:

```
hostname(config)# l2tp tunnel hello 30
```

Related Commands

Command	Description
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	Displays the details of L2TP connections.
vpn-tunnel-protocol l2tp-ipsec	Enables L2TP as a tunneling protocol for a specific tunnel group.

ldap attribute-map

To create and name an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names, use the **ldap attribute-map** command in global configuration mode. To remove the map, use the **no** form of this command.

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

Syntax Description

map-name	Specifies a user-defined name for an LDAP attribute map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **ldap attribute-map** command, you can map your own attribute names and values to Cisco attribute names. You can then bind the resulting attribute map to an LDAP server. Your typical steps would be as follows:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after ldap in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example command, entered in global configuration mode, creates an LDAP attribute map named myldapmap prior to populating it or binding it to an LDAP server:

```
hostname(config)# ldap attribute-map myldapmap
```

```
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name to a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to the Cisco attribute name.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

ldap-attribute-map (aaa-server host mode)

To bind an existing mapping configuration to an LDAP host, use the **ldap-attribute-map** command in aaa-server host configuration mode. To remove the binding, use the **no** form of this command.

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

Syntax Description

map-name	Specifies an LDAP attribute mapping configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

If the Cisco-defined LDAP attribute names do not meet your ease-of-use or other requirements, you can create your own attribute names, map them to Cisco attributes, and then bind the resulting attribute configuration to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This command enters ldap-attribute-map mode. Note that there is no hyphen after "ldap" in this command.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute mapping configuration.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map configuration to an LDAP server.

Examples

The following example commands, entered in aaa-server host configuration mode, bind an existing attribute map named myldapmap to an LDAP server named ldapsvr1:

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running ldap attribute mapping configuration or all running attribute mapping configurations.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

ldap-base-dn

To specify the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request, use the **ldap-base-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, thus resetting the search to start at the top of the list, use the **no** form of this command.

ldap-base-dn *string*

no ldap-base-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request; for example, OU=Cisco. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

Start the search at the top of the list.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Pre-existing command, modified for this release

Usage Guidelines

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP base DN as starthere.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN.

ldap-defaults

To define LDAP default values, use the **ldap-defaults** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These default values are used only when the LDAP server requires them. To specify no LDAP defaults, use the **no** form of this command.

ldap-defaults *server* [*port*]

no ldap-defaults

Syntax Description

port	(Optional) Specifies the LDAP server port. If this parameter is not specified, the security appliance uses the standard LDAP port (389).
server	Specifies the IP address or domain name of the LDAP server. If one exists within the CRL distribution point, it overrides this value.

Defaults

The default setting is not set.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example defines LDAP default values on the default port (389):

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs

ldap-dn

To pass a X.500 distinguished name and password to an LDAP server that requires authentication for CRL retrieval, use the **ldap-dn** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them. To specify no LDAP DN, use the **no** form of this command.

ldap-dn *x.500-name password*

no ldap-dn

Syntax Description

password	Defines a password for this distinguished name. The maximum field length is 128 characters.
x.500-name	Defines the directory path to access this CRL database, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum field length is 128 characters.

Defaults

The default setting is not on.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crl configure configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example specifies an X.500 name CN=admin,OU=devtest,O=engineering and a password xxzzyy for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

Related Commands

Command	Description
crl configure	Enters crl configure configuration mode.
crypto ca trustpoint	Enters ca trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

ldap-group-base-dn

To specify the base group in the Active Directory hierarchy used by dynamic access policies for group searches, use the **ldap-group-base-dn** command in aaa-server host configuration mode. To remove the command from the running configuration, use the **no** form of the command:

ldap-group-base-dn [*string*]

no ldap-group-base-dn [*string*]

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the location in the Active Directory hierarchy where the server should begin searching. For example, ou=Employees. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behavior or values. If you do not specify a group search DN, the search begins at the base DN.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **ldap-group-base-dn** command applies only to Active Directory servers using LDAP, and specifies an Active Directory heirarchy level that the **show ad-groups** command uses to begin its group search. The groups retrieved from the search are used by dynamic group policies as selection criteria for a specific policy.

Examples

The following example sets the group base DN to begin the search at the organization unit (ou) level Employees:

```
hostname(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

Related Commands

Command	Description
group-search-timeout	Adjusts the time the security appliance waits for a response from an Active Directory server for a list of groups.
show ad-groups	Displays groups that are listed on an Active Directory server.

ldap-login-dn

To specify the name of the directory object that the system should bind this as, use the **ldap-login-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-login-dn *string*

no ldap-login-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Some LDAP servers, including the Microsoft Active Directory server, require that the security applianceestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the security appliance. These characteristics should correspond to those of a user with administrator privileges.

For the *string* variable, enter the name of the directory object for VPN Concentrator authenticated binding, for example: cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com. For anonymous access, leave this field blank.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login DN as myobjectname.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
```

```
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-login-password

To specify the login password for the LDAP server, use the **ldap-login-password** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this password specification, use the **no** form of this command:

ldap-login-password *string*

no ldap-login-password

Syntax Description

string	A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum password string length is 64 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login password as obscurepassword.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-naming-attribute

To specify the Relative Distinguished Name attribute, use the **ldap-naming-attribute** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-naming-attribute *string*

no ldap-naming-attribute

Syntax Description

string	The case-sensitive, alphanumeric Relative Distinguished Name attribute, consisting of up to 128 characters, that uniquely identifies an entry on the LDAP server. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Examples

The following example configures an LDAP AAA server named srvgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP naming attribute as cn.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-over-ssl

To establish a secure SSL connection between the security appliance and the LDAP server, use the **ldap-over-ssl** command in aaa-server host configuration mode. To disable SSL for the connection, use the **no** form of this command.

ldap-over-ssl enable

no ldap-over-ssl enable

Syntax Description

enable	Specifies that SSL secures a connection to an LDAP server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to specify that SSL secures a connection between the security appliance and an LDAP server.

Note We recommend enabling this feature if you are using plain text authentication. See the **sasl-mechanism** command.

Examples

The following commands, entered in aaa-server host configuration mode, enable SSL for a connection between the security appliance and the LDAP server named ldapsvr1 at IP address 10.10.0.1. They also configure the plain SASL authentication mechanism.

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
sasl-mechanism	Specifies SASL authentication between the LDAP client and server.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

ldap-scope

To specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request, use the **ldap-scope** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-scope *scope*

no ldap-scope

Syntax Description

scope	The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values are: • **onelevel**—Search only one level beneath the Base DN • **subtree**—Search all levels beneath the Base DN

Defaults

The default value is **onelevel**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Pre-existing command, modified for this release

Usage Guidelines

Specifying the scope as **onelevel** results in a faster search, because only one level beneath the Base DN is searched. Specifying **subtree** is slower, because all levels beneath the Base DN are searched.

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named svrgrp1 on host 1.2.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP scope to include the subtree levels.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN. This command is valid only for LDAP servers.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.

leap-bypass

To enable LEAP Bypass, use the **leap-bypass enable** command in group-policy configuration mode. To disable LEAP Bypass, use the **leap-bypass disable** command. To remove the LEAP Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for LEAP Bypass from another group policy.

leap-bypass {**enable | disable**}

no leap-bypass

Syntax Description

disable	Disables LEAP Bypass.
enable	Enables LEAP Bypass.

Defaults

LEAP Bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When enabled, LEAP Bypass allows LEAP packets from wireless devices behind a VPN hardware client to travel across a VPN tunnel prior to user authentication. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Devices are then able to authenticate again, per user authentication.

This feature does not work as intended if you enable interactive hardware client authentication.

For further information, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Note There may be security risks in allowing any unauthenticated traffic to traverse the tunnel.

Examples

The following example shows how to set LEAP Bypass for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

Related Commands

Command	Description
secure-unit-authentication	Requires VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel.
user-authentication	Requires users behind VPN hardware clients to identify themselves to the security appliance before connecting.

lifetime (ca server mode)

To specify the length of time that the Local Certificate Authority (CA) certificate, each issued user certificates, or the Certificate Revocation List (CRL) is valid, use the **lifetime** command in CA server configuration mode. To reset the lifetime to the default setting, use the **no** form of this command.

lifetime {ca-certificate | **certificate | crl**} *time*

no lifetime {**ca-certificate** | **certificate | crl**}

Syntax Description

ca-certificate	Specifies the lifetime of the local CA server certificate.
certificate	Specifies the lifetime of all user certificates issued by the CA server.
crl	Specifies the lifetime of the CRL.
time	For the CA certificate and all issued certificates, *time* specifies the number of days the certificate is valid. The valid range is from 1 to 3650 days. For the CRL, *time* specifies the number of hours the CRL is valid. The valid range for the CRL is from 1 to 720 hours.

Defaults

The default lifetimes are:

- CA certificate - Three years
- Issued certificates - One year
- CRL - Six hours

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

By specifying the number of days or hours that a certificate or CRL is valid, this command determines the expiration date included in the certificate or the CRL.

Examples

The following example configures the CA to issue certificates that are valid for three months:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime certificate 90
```

```
hostname(config-ca-server))#
```

The following example configures the CA to issue a CRL that is valid for two days:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# lifetime crl 48
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies the certificate revocation list distribution point (CDP) to be include in the certificates issued by the CA.
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
show crypto ca server	Displays the local CA configuration details in ASCII text.
show crypto ca server cert-db	Displays local CA server certificates.
show crypto ca server crl	Displays the current CRL of the local CA.

limit-resource

To specify a resource limit for a class in multiple context mode, use the **limit-resource** command in class configuration mode. To restore the limit to the default, use the **no** form of this command. The security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

limit-resource {**all 0** | [**rate**] *resource_name number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

Syntax Description

all 0	Sets the limit for all resources as unlimited.
number[**%**]	Specifies the resource limit as a fixed number greater than or equal to 1, or as a percentage of the system limit between 1 and 100 (when used with the percent sign (%)). Set the limit to **0** to indicate an unlimited resource. For resources that do not have a system limit, you cannot set the percentage (%); you can only set an absolute value.
rate	Specifies that you want to set the rate per second for a resource. See Table 18-1 for resources for which you can set the rate per second.
resource_name	Specifies the resource name for which you want to set a limit. This limit overrides the limit set for **all**.

Defaults

All resources are set to unlimited, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- IPSec sessions—5 sessions.
- MAC addresses—65,535 entries.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you limit a resource for a class, the security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the security appliance sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can "use up" those resources, potentially affecting service to other contexts.

Table 18-1 lists the resource types and the limits. See also the **show resource types** command.

Table 18-1 Resource Names and Limits

Resource Name	Rate or Concurrent	Minimum and Maximum Number per Context	System Limit[1]	Description
mac-addresses	Concurrent	N/A	65,535	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	Concurrent or Rate	N/A	Concurrent connections: See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for the connection limit for your platform. Rate: N/A	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
inspects	Rate	N/A	N/A	Application inspections.
hosts	Concurrent	N/A	N/A	Hosts that can connect through the security appliance.
asdm	Concurrent	1 minimum 5 maximum	32	ASDM management sessions. **Note** ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 ASDM sessions represents a limit of 64 HTTPS sessions.
ssh	Concurrent	1 minimum 5 maximum	100	SSH sessions.
syslogs	Rate	N/A	N/A	System log messages.
telnet	Concurrent	1 minimum 5 maximum	100	Telnet sessions.
xlates	Concurrent	N/A	N/A	Address translations.

1. If this column value is N/A, then you cannot set a percentage of the resource because there is no hard system limit for the resource.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
member	Assigns a context to a resource class.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

lmfactor

To set a revalidation policy for caching objects that have only the last-modified timestamp, and no other server-set expiration values, use the **lmfactor** command in cache configuration mode. To set a new policy for revalidating such objects, use the command again. To reset the attribute to the default value of 20, enter the **no** version of the command.

lmfactor *value*

no lmfactor

Syntax Description

value	An integer in the range of 0 to 100.

Defaults

The default value is 20.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cache configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The security appliance uses the value of the lmfactor to estimate the length of time for which it considers a cached object to be unchanged. This is known as the expiration time. The security appliance estimates th expiration time by the time elapsed since the last modification multiplied by the lmfactor.

Setting the lmfactor to zero is equivalent to forcing an immediate revalidation, while setting it to 100 results in the longest allowable time until revalidation.

Examples

The following example shows how to set an lmfactor of 30:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

log

When using the Modular Policy Framework, log packets that match a **match** command or class map by using the **log** command in match or class configuration mode. This log action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic. To disable this action, use the **no** form of this command.

log

no log

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **log** command to log all packets that match the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example sends a log when packets match the http-traffic class map.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

log-adj-changes

To configure the router to send a syslog message when an OSPF neighbor goes up or down, use the **log-adj-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **log-adj-changes** command is enabled by default; it appears in the running configuration unless removed with the **no** form of the command.

Examples

The following example disables the sending of a syslog message when an OSPF neighbor goes up or down:

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.

CHAPTER 19

logging asdm through logout message Commands

logging asdm

To send system log messages to the ASDM log buffer, use the **logging asdm** command in global configuration mode. To disable logging to the ASDM log buffer, use the **no** form of this command.

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the ASDM log buffer. For information about creating lists, see the **logging list** command.

Defaults

ASDM logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Before any messages are sent to the ASDM log buffer, you must enable logging using the **logging enable** command.

When the ASDM log buffer is full, security appliance deletes the oldest message to make room in the buffer for new messages. To control the number of system log messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

This example shows how to enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages it contains.
logging asdm-buffer-size	Specifies the number of ASDM messages retained in the ASDM log buffer
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging configuration.

logging asdm-buffer-size

To specify the number of system log messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command in global configuration mode. To reset the ASDM log buffer to its default size of 100 messages, use the **no** form of this command.

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

Syntax Description

num_of_msgs	Specifies the number of system log messages that the security appliance retains in the ASDM log buffer.

Defaults

The default ASDM syslog buffer size is 100 messages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When the ASDM log buffer is full, security appliance deletes the oldest message to make room in the buffer for new messages. To control whether logging to the ASDM log buffer is enabled or to control the kind of system log messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

This example shows how enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages it contains.
logging asdm	Enables logging to the ASDM log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffered

To enable the security appliance to send system log messages to the log buffer, use the **logging buffered** command in global configuration mode. To disable logging to the log buffer, use the **no** form of this command.

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the log buffer. For information about creating lists, see the **logging list** command.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Buffer size is 4 KB.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the log buffer, you must enable logging using the **logging enable** command.

New messages append to the end of the buffer. When the buffer fills up, the security appliance clears it and continues adding messages to it. When the log buffer is full, the security appliance deletes the oldest message to make room in the buffer for new messages. You can have buffer contents automatically saved each time the contents of the buffer have “wrapped”, which means that all the messages since the last save have been replaced by new messages. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

At any time, you can save the contents of the buffer to Flash memory. For more information, see the **logging savelog** command.

System log messages sent to the buffer can be viewed with the **show logging** command.

Examples

This example configures logging to the buffer for level 0 and level 1 events:

```
hostname(config)# logging buffered alerts
hostname(config)#
```

This example creates a list named notif-list with a maximum logging level of 7 and configures logging to the buffer for system log messages identified by the notif-list list.

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages that it contains.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.
logging list	Creates a reusable list of message selection criteria.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffer-size

To specify the size of the log buffer, use the **logging buffer-size** command in global configuration mode. To reset the log buffer to its default size of 4 KB of memory, use the **no** form of this command.

logging buffer-size *bytes*

no logging buffer-size *bytes*

Syntax Description

bytes	Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the security appliance uses 8 KB of memory for the log buffer.

Defaults

The log buffer size is 4 KB of memory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see whether the security appliance is using a log buffer of a size other than the default buffer size, use the **show running-config logging** command. If the **logging buffer-size** command is not shown, then the security appliance uses a log buffer of 4 KB.

For more information about how the security appliance uses the buffer, see the **logging buffered** command.

Examples

This example enables logging, enables the logging buffer, and specifies that the security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging class

To configure the maximum logging level per logging destination for a message class, use the **logging class** command in global configuration mode. To remove a message class logging level configuration, use the **no** form of the command.

logging class *class destination level* [*destination level . . .*]

no logging class *class*

Syntax Description

class	Specifies the message class whose maximum logging levels per destination. For valid values of class, see the "Usage Guidelines" section that follows.
destination	Specifies a logging destination for *class*. For the destination, the *level* determines the maximum logging level sent to *destination*. For valid values of *destination*, see the "Usage Guidelines" section that follows.
level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.

Defaults

By default, the security appliance does not apply logging levels on a logging destination and message class basis. Instead, each enabled logging destination receives messages for all classes at the logging level determined by the logging list or level specified when you enabled the logging destination.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Added **eigrp** to valid class values.

Usage Guidelines

Valid values for *class* include the following:

- **auth**—User authentication.
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **eigrp**—EIGRP routing.
- **email**—Email proxy.
- **ha**—Failover.
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.
- **ospf**—OSPF routing.
- **rip**—RIP routing.
- **session**—User session.
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPSec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Valid logging destinations are as follows:

- **asdm**—To learn about this destination, see the **logging asdm** command.
- **buffered**—To learn about this destination, see the **logging buffered** command.
- **console**—To learn about this destination, see the **logging console** command.
- **history**—To learn about this destination, see the **logging history** command.
- **mail**—To learn about this destination, see the **logging mail** command.

- **monitor**—To learn about this destination, see the **logging monitor** command.
- **trap**—To learn about this destination, see the **logging trap** command.

Examples

This example specifies that, for failover-related messages, the maximum logging level for the ASDM log buffer is 2 and the maximum logging level for the system log buffer is 7:

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging console

To enable the security appliance to display system log messages in console sessions, use the **logging console** command in global configuration mode. To disable the display of system log messages in console sessions, use the **no** form of this command.

logging console [*logging_list* | *level*]

no logging console

Note We recommend that you do not use this command because it may cause many system log messages to be dropped due to buffer overflow. For more information, see the "Usage Guidelines" section that follows.

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the console session. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not display system log messages in console sessions by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the console, you must enable logging using the **logging enable** command.

Caution Using the **logging console** command could significantly degrade system performance. Instead, use the **logging buffered** command to start logging and the **show logging** command to view the messages. To make viewing the most current messages easier, use the **clear logging buffer** command to clear the buffer.

Examples

This example shows how to enable system log messages of levels 0, 1, 2, and 3 to appear in console sessions:

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging debug-trace

To redirect debugging messages to logs as system log message 711001 issued at severity level 7, use the **logging debug-trace** command in global configuration mode. To stop sending debugging messages to logs, use the **no** form of this command.

logging debug-trace

no logging debug-trace

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not include debug output in system log messages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Debug messages are generated as severity level 7 messages. They appear in logs with the system log message number 711001, but do not appear in any monitoring session.

Examples

This example shows how to enable logging, send log messages to the system log buffer, redirect debugging output to logs, and turn on debugging disk activity.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

An example of a debug message that could appear in the logs follows:

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging device-id

To configure the security appliance to include a device ID in non-EMBLEM-format system log messages, use the **logging device-id** command in global configuration mode. To disable the use of a device ID, use the **no** form of this command.

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

Syntax Description

context-name	Specifies the name of the current context as the device ID.
hostname	Specifies the hostname of the security appliance as the device ID.
ipaddress *interface_name*	Specifies the device ID or the IP address of the interface in *interface_name*. If you use the **ipaddress** keyword, system log messages sent to an external server contain the IP address of the interface specified, regardless of which interface the security appliance uses to send the log data to the external server.
string *text*	Specifies as the device ID the characters contained in *text*, which can be up to 16 characters long. You cannot use white space characters or any of the following characters: • &—ampersand • '—single quote • "—double quote • <—less than • >—greater than • ?—question mark

Defaults

No default device ID is used in system log messages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you use the **ipaddress** keyword, the device ID becomes the specified security appliance interface IP address, regardless of the interface from which the message is sent. This keyword provides a single, consistent device ID for all messages that are sent from the device.

Examples

This example shows how to configure a host named secappl-1:

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

The host name appears at the beginning of system log messages, such as in the following message:

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging emblem

To use the EMBLEM format for system log messages sent to destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of EMBLEM format, use the **no** form of this command.

logging emblem

no logging emblem

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not use EMBLEM format for system log messages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed to be independent of the **logging host** command.

Usage Guidelines

The **logging emblem** command lets you to enable EMBLEM-format logging for all logging destinations other than syslog servers. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

Examples

This example shows how to enable logging and enable the use of EMBLEM-format for logging to all logging destinations except syslog servers:

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging enable

To enable logging for all configured output locations, use the **logging enable** command in global configuration mode. To disable logging, use the **no** form of this command.

logging enable

no logging enable

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **logging on** command.

Usage Guidelines

The **logging enable** command allows you to enable or disable sending system log messages to any of the supported logging destinations. You can stop all logging with the **no logging enable** command.

You can enable logging to individual logging destinations with the following commands:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Examples

This example shows how to enable logging. The output of the **show logging** command illustrates how each possible logging destination must be enabled separately.

```
hostname(config)# logging enable
hostname(config)# show logging
Syslog logging: enabled
```

```
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Deny Conn when Queue Full: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging facility

To specify the logging facility used for messages sent to syslog servers, use the **logging facility** command in global configuration mode. To reset the logging facility to its default of 20, use the **no** form of this command.

logging facility *facility*

no logging facility

Syntax Description

facility	Specifies the logging facility; valid values are 16 through 23.

Defaults

The default facility is 20 (LOCAL4).

Command Modes

The following table shows the modes in which you can enter the command, with the exceptions noted in the Syntax Description section:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Syslog servers file messages based on the *facility* number in the message. There are eight possible facilities: 16 (LOCAL0) through 23 (LOCAL7).

Examples

This example shows how to specify that the security appliance specify the logging facility as 16 in system log messages. The output of the **show logging** command includes the facility being used by the security appliance.

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
```

```
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging flash-bufferwrap

To enable the security appliance to write the log buffer to Flash memory every time the buffer is full of messages that have never been saved, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing of the log buffer to Flash memory, use the **no** form of this command.

logging flash-bufferwrap

no logging flash-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Writing the log buffer to Flash memory is disabled.
- Buffer size is 4 KB.
- Minimum free Flash memory is 3 MB.
- Maximum Flash memory allocation for buffer logging is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

For the security appliance to write the log buffer to Flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

While the security appliance writes log buffer contents to Flash memory, it continues storing to the log buffer continues any new event messages.

The security appliance creates log files with names that use a default time-stamp format, as follows:

LOG-*YYYY-MM-DD-HHMMSS*.TXT

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

The availability of Flash memory affects how the security appliance saves system log messages using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

Examples

This example shows how to enable logging, enable the log buffer, and enable the security appliance to write the log buffer to Flash memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging flash-maximum-allocation	Specifies the maximum amount of Flash memory that can be used for writing log buffer contents.
logging flash-minimum-free	Specifies the minimum amount of Flash memory that must be available for the security appliance to permit writing of the log buffer to Flash memory.
show logging	Displays the enabled logging options.

logging flash-maximum-allocation

To specify the maximum amount of Flash memory that the security appliance uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. To reset the maximum amount of Flash memory used for this purpose to its default size of 1 MB of Flash memory, use the **no** form of this command.

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

Syntax Description

kbytes	The largest amount of Flash memory, in kilobytes, that the security appliance can use to save log buffer data.

Defaults

The default maximum Flash memory allocation for log data is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command determines how much Flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** causes Flash memory use for log files to exceed the maximum amount specified by the **logging flash-maximum-allocation** command, the security appliance deletes the oldest log files to free sufficient memory for the new log file. If there are no files to delete or if, after all old files are deleted, free memory is too small for the new log file, the security appliance fails to save the new log file.

To see whether the security appliance has a maximum Flash memory allocation of a size different than the default size, use the **show running-config logging** command. If the **logging flash-maximum-allocation** command is not shown, then the security appliance uses a maximum of 1 MB for saved log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the security appliance uses the log buffer, see the **logging buffered** command.

Examples

This example shows how to enable logging, enable the log buffer, enable the security appliance to write the log buffer to Flash memory, with the maximum amount of Flash memory used for writing log files set to approximately 1.2 MB of memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging flash-minimum-free	Specifies the minimum amount of Flash memory that must be available for the security appliance to permit writing of the log buffer to Flash memory.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging flash-minimum-free

To specify the minimum amount of free Flash memory that must exist before the security appliance saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. This command affects how much free Flash memory must exist before the security appliance saves log files created by the **logging savelog** and **logging flash-bufferwrap** commands. To reset the minimum required amount of free Flash memory to its default size of 3 MB, use the **no** form of this command.

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

Syntax Description

kbytes	The minimum amount of Flash memory, in kilobytes, that must be available before the security appliance saves a new log file.

Defaults

The default minimum free Flash memory is 3 MB.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The logging flash-minimum-free command specifies how much Flash memory the **logging savelog** and **logging flash-bufferwrap** commands must preserve at all times.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** would cause the amount of free Flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the security appliance fails to save the new log file.

Examples

This example shows how to enable logging, enable the log buffer, enable the security appliance to write the log buffer to Flash memory, and specifies that the minimum amount of free Flash memory must be 4000 KB:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
```

```
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging flash-maximum-allocation	Specifies the maximum amount of Flash memory that can be used for writing log buffer contents.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging from-address

To specify the sender e-mail address for system log messages sent by the security appliance, use the **logging from-address** command in global configuration mode. All sent system log messages appear to come from the address you specify. To remove the sender e-mail address, use the **no** form of this command.

logging from-address *from-email-address*

no logging from-address *from-email-address*

Syntax Description

from-email-address	Source e-mail address, that is, the e-mail address that system log messages appear to come from (for example, cdb@example.com).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Sending system log messages by e-mail is enabled by the **logging mail** command.

The address specified with this command need not correspond to an existing e-mail account.

Examples

To enable logging and set up the security appliance to send system log messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
```

```
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging mail	Enables the security appliance to send system log messages by e-mail and determines which messages are sent by e-mail.
logging recipient-address	Specifies the e-mail address to which system log messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging ftp-bufferwrap

To enable the security appliance to send the log buffer to an FTP server every time the buffer is full of messages that have never been saved, use the **logging ftp-bufferwrap** command in global configuration mode. To disable sending the log buffer to an FTP server, use the **no** form of this command.

logging ftp-bufferwrap

no logging ftp-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Sending the log buffer to an FTP server is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you enable **logging ftp-bufferwrap**, the security appliance sends log buffer data to the FTP server you specify with the **logging ftp-server** command. While the security appliance sends log data to the FTP server, it continues storing to the log buffer continues any new event messages.

For the security appliance to send log buffer contents to an FTP server, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

The security appliance creates log files with names that use a default time-stamp format, as follows:

LOG-*YYYY-MM-DD-HHMMSS*.TXT

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Examples

This example shows how enable logging, enable the log buffer, specify an FTP server, and enable the security appliance to write the log buffer to an FTP server. This example specifies an FTP server whose host name is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the /syslogs directory.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-server	Specifies FTP server parameters for use with the **logging ftp-bufferwrap** command.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging ftp-server

To specify details about the FTP server that the security appliance sends log buffer data to when **logging ftp-bufferwrap** is enabled, use the **logging ftp-server** command in global configuration mode. To remove all details about an FTP server, use the **no** form of this command.

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) user password will follow.
8	(Optional) Specifies that an encrypted user password will follow.
ftp-server	External FTP server IP address or hostname. **Note** If you specify a hostname, be sure DNS is operating correctly on your network.
password	The password for the username specified.
path	Directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. For example: `/security_appliances/syslogs/appliance107`
username	A username that is valid for logging in to the FTP server.

Defaults

No FTP server is specified by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(5)	Support for password encryption was added.

Usage Guidelines

You can only specify one FTP server. If a logging FTP server is already specified, using the **logging ftp-server** command replaces that FTP server configuration with the new one you enter.

The security appliance does not verify the FTP server information you specify. If you misconfigure any of the details, the security appliance fails to send log buffer data to the FTP server.

During bootup or upgrade of the security appliance, single-digit passwords and passwords startingwith a digit followed by a whitespace are not supported. For example, 0 pass and 1 are invalid passwords.

Examples

This example shows how to enable logging, enable the log buffer, specify an FTP server, and enable the security appliance to write the log buffer to an FTP server. This example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the /syslogs directory.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
```

The following example shows how to enter an encrypted password:

```
hostname(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

The following example shows how to enter an unencrypted (clear text) password:

```
hostname(config)# logging ftp-server logserver /path1 user1 0 pass1
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging history

To enable SNMP logging and specify which messages are to be sent to SNMP servers, use the **logging history** command in global configuration mode. To disable SNMP logging, use the **no** form of this command.

logging history [*logging_list* | *level*]

no logging history

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the SNMP server. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not log to SNMP servers by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging history** command allows you to enable logging to an SNMP server and to set the SNMP message level or event list.

Examples

This example shows how to enable SNMP logging and specify that messages of levels 0, 1, 2, and 3 are sent to the SNMP server configured:

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
snmp-server	Specifies SNMP server details.

logging host

To define a syslog server, use the **logging host** command in global configuration mode. To remove a syslog server definition, use the **no** form of this command.

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**] [**permit-hostdown**]

logging host *interface_name syslog_ip*

[**no**] **logging host** *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**]

[**no**] **logging host** *interface_name syslog_ip*

Syntax Description

format emblem	(Optional) Enables EMBLEM format logging for the syslog server.
interface_name	Specifies the interface on which the syslog server resides.
permit-hostdown	Allows the adaptive security appliance to continue TCP logging when the syslog server is down or unreachable.
port	Indicates the port that the syslog server listens to for messages. Valid port values are 1025 through 65535 for either protocol.
secure	Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. **Note** A secure logging connection can only be established with a SSL/TLS-capable syslog server. If a SSL/TLS connection cannot be established, all new connections will be denied. You may change this default behavior by entering the **logging permit-hostdown** command.
syslog_ip	Specifies the IP address of the syslog server.
tcp	Specifies that the adaptive security appliance should use TCP to send messages to the syslog server.
udp	Specifies that the adaptive security appliance should use UDP to send messages to the syslog server.

Defaults

The default protocol is UDP.

The default port numbers are as follows:

- UDP—514
- TCP —1470

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.
8.0(2)	The **secure** keyword was added.

Usage Guidelines

The **logging host** *ip_address* **format emblem** command allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP system log messages only. If you enable EMBLEM-format logging for a particular syslog server, then the messages are sent to that server. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

You can use multiple **logging host** commands to specify additional servers that would all receive the system log messages. However, you can only specify a server to receive either UDP or TCP system log messages, not both.

Note When the **tcp** option is used in the **logging host** command, the adaptive security appliance will drop connections across the firewall if the syslog server is unreachable.

You can display only the *port* and *protocol* values that you previously entered by using the **show running-config logging** command and finding the command in the listing—TCP is listed as 6 and UDP is listed as 17. TCP ports work only with the syslog server. The *port* must be the same port on which the syslog server listens.

Note An error message occurs if you try to use the **logging host** command and the **secure** keyword with UDP.

The PIX security appliance does not support the **secure** keyword.

Examples

This example shows how to send system log messages of severity levels 0, 1, 2, and 3 to a syslog server on the inside interface that uses the default protocol and port number.

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging list

To create a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs), use the **logging list** command in global configuration mode. To remove the list, use the **no** form of this command.

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

Syntax Description

class *event_class*	(Optional) Sets the class of events for system log messages. For the level specified, only system log messages of the class specified are identified by the command. See the "Usage Guidelines" section for a list of classes.
level *level*	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
message *start_id*[**-***end_id*]	Specified a message ID or range of IDs. To look up the default level of a message, use the **show logging** command or see the *Cisco ASA 5500 Series System Log Messages*.
name	Sets the logging list name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Logging commands that can use lists are the following:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *event_class* include the following:

- **auth**—User authentication.
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **email**—-Email proxy.
- **ha**—Failover.
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.
- **ospf**—OSPF routing.
- **rip**—RIP routing.
- **session**—User session.
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPSec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Examples

This example shows how to use the logging list command:

```
hostname(config)# logging list my-list message 100100-100110
hostname(config)# logging list my-list level critical
```

```
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

The preceding example states that system log messages that match the criteria specified will be sent to the logging buffer. The criteria specified in this example are:

- System log message IDs that fall in the range of 100100 to 100110
- All system log messages with a critical level or higher (emergency, alert, or critical)
- All VPN class system log messages with a warning level or higher (emergency, alert, critical, error, or warning)

If a system log message satisfies any one of these conditions, it is logged to the buffer.

Note When you design list criteria, criteria can specify overlapping sets of messages. System log messages matching more than one set of criteria are logged normally.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging mail

To enable the security appliance to send system log messages by e-mail and to determine which messages are sent by e-mail, use the **logging mail** command in global configuration mode. To disable e-mailing of system log messages, use the **no** form of this command.

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the e-mail recipient. For information about creating lists, see the **logging list** command.

Defaults

Logging to e-mail is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

E-mailed system log messages appear in the subject line of the e-mails sent.

Examples

To set up the security appliance to send system log messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which e-mailed system log messages appear to come.
logging list	Creates a reusable list of message selection criteria.
logging recipient-address	Specifies the e-mail address to which e-mailed system log messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging message

To specify the logging level of a system log message, use the **logging message** command with the **level** keyword in global configuration mode. To reset the logging level of a message to its default level, use the **no** form of this command. To prevent the security appliance from generating a particular system log message, use the **no** form of the **logging message** command (without the **level** keyword) in global configuration mode. To let the security appliance generate a particular system log message, use the **logging message** command (without the **level** keyword). These two versions of the **logging message** command can be used in parallel. See the "Examples" section that follows.

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

Syntax Description

level *level*	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
syslog_id	The ID of the system log message that you want to enable or disable or whose severity level you want to modify. To look up the default level of a message, use the **show logging** command or see the *Cisco ASA 5500 Series System Log Messages*.

Defaults

By default, all system log messages are enabled and the severity levels of all messages are set to their default levels.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can use the **logging message** command for two purposes:

- To control whether a message is enabled or disabled.
- To control the severity level of a message.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

Examples

The series of commands in the following example illustrate the use of the **logging message** command to control both whether a message is enabled and the severity level of the messages:

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

Command	Description
clear configure logging	Clears all logging configuration or message configuration only.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging monitor

To enable the security appliance to display system log messages in SSH and Telnet sessions, use the **logging monitor** command in global configuration mode. To disable the display of system log messages in SSH and Telnet sessions, use the **no** form of this command.

logging monitor [*logging_list* | *level*]

no logging monitor

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the SSH or Telnet session. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not display system log messages in SSH and Telnet sessions by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging monitor** command enables system log messages for all sessions in the current context; however, in each session, the **terminal** command controls whether system log messages appear in that session.

Examples

This example shows how to enable the display of system log messages in console sessions. The use of the **errors** keyword indicates that messages of levels 0, 1, 2, and 3 should display in SSH and Telnet sessions. The **terminal** command enables the messages to appear in the current session.

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
terminal	Sets terminal line parameters.

logging permit-hostdown

To make the status of a TCP-based syslog server irrelevant to new user sessions, use the **logging permit-hostdown** command in global configuration mode. To cause the security appliance to deny new user sessions when a TCP-based syslog server is unavailable, use the **no** form of this command.

logging permit-hostdown

no logging permit-hostdown

Syntax Description

This command has no arguments or keywords.

Defaults

By default, if you have enabled logging to a syslog server that uses a TCP connection, the security appliance does not allow new network access sessions when the syslog server is unavailable for any reason.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you are using TCP as the logging transport protocol for sending messages to a syslog server, the security appliance denies new network access sessions as a security measure if the security appliance is unable to reach the syslog server. You can use the **logging permit-hostdown** command to remove this restriction.

Examples

The following example makes the status of TCP-based syslog servers irrelevant to whether the security appliance permits new sessions. When the **logging permit-hostdown** command includes in its output the **show running-config logging** command, the status of TCP-based syslog servers is irrelevant to new network access sessions.

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging queue

To specify how many system log messages the security appliance may hold in its queue before processing them according to the logging configuration, use the **logging queue** command in global configuration mode. To reset the logging queue size to the default of 512 messages, use the **no** form of this command.

logging queue *queue_size*

no logging queue *queue_size*

Syntax Description

queue_size	The number of system log messages permitted in the queue used for storing system log messages before processing them. Valid values are from 0 to 8192 messages. If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages).

Defaults

The default queue size is 512 messages.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When traffic is so heavy that the queue fills up, the security appliance may discard messages.

Examples

This example shows how to display the output of the **logging queue** and **show logging queue** commands:

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the **logging queue** command is set to 0, which means that the queue is set to the maximum of 8192. The system log messages in the queue are processed by the security appliance in the manner dictated by the logging configuration, such as sending system log messages to mail recipients, saving them to Flash memory, and so forth.

The output of this example **show logging queue** command shows that 5 messages are queued, 3513 messages was the largest number of messages in the queue at one time since the security appliance was last booted, and that 1 message was discarded. Even though the queue was set for unlimited, the messages was discarded because no block memory was available to add the message to the queue.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging rate-limit

To limit the rate at which system log messages are generated, use the **logging rate-limit** command in privileged EXEC mode. To disable rate limiting, use the **no** form of this command in privileged EXEC mode.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

Syntax Description

interval	(Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for *interval* is 0 through 2147483647.
level *severity_level*	Applies the set rate limits on all system log messages that belong to a certain severity level. All system log messages at a specified severity level are rate-limited individually. The valid range for *severity_level* is 1 through 7.
message	Suppresses reporting of this system log message.
num	Number of system messages that can be generated during the specified time interval. The valid range of values for *num* is 0 through 2147483647.
syslog_id	ID of the system log message to be suppressed. The valid range of values is 100000-999999.
unlimited	Disables rate limiting, which means that there is no limit on the logging rate.

Defaults

The default setting for *interval* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The system message severity levels are as follows:

•0—System Unusable

•1—Take Immediate Action

•2—Critical Condition

•3—Error Message

- 4—Warning Message
- 5—Normal but significant condition
- 6—Informational
- 7—Debug Message

Examples

To limit the rate of system log message generation, you can enter a specific message ID. The following example shows how to limit the rate of system log message generation using a specific message ID and time interval:

```
hostname(config)# logging rate-limit 100 600 message 302020
```

This example suppresses system log message 302020 from being sent to the host after the rate limit of 100 is reached in the specified interval of 600 seconds.

To limit the rate of system log message generation, you can enter a specific severity level. The following example shows how to limit the rate of system log message generation using a specific severity level and time interval.

```
hostname(config)# logging rate-limit 1000 600 level 6
```

This example suppresses all system log messages under severity level 6 to the specified rate limit of 1000 in the specified time interval of 600 seconds. Each system log message in severity level 6 has a rate limit of 1000.

Related Commands

Command	Description
clear running-config logging rate-limit	Resets the logging rate limit setting to its default.
show logging	Shows the messages currently in the internal buffer or to shows logging configuration settings.
show running-config logging rate-limit	Shows the current logging rate limit setting.

logging recipient-address

To specify the receiving e-mail address for system log messages sent by the security appliance, use the **logging recipient-address** command in global configuration mode. To remove the receiving e-mail address, use the **no** form of this command. You can configure up to 5 recipient addresses. If you want, each recipient address can have a different message level than that specified by the **logging mail** command.

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

Syntax Description

address	Specifies recipient e-mail address when sending system log messages by -email.
level	Indicates that a logging level follows.
level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs. **Note** We do not recommend using a level greater than 3 with the **logging recipient-address** command. Higher logging levels are likely to cause dropped system log messages because of buffer overflow. The message level specified by a **logging recipient-address** command overrides the message level specified by the **logging mail** command. For example, if a **logging recipient-address** command specifies a level of 7 but the **logging mail** command specifies a level of 3, the security appliance sends all messages to the recipient, including those of levels 4, 5, 6, and 7.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	Multiple System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Sending system log messages by e-mail is enabled by the **logging mail** command.

You can configure up to 5 **logging recipient-address** commands. Each command can have a different logging level than the others. This command is useful when you want more urgent messages to go to a larger number of recipients than less urgent messages are sent to.

Examples

To set up the security appliance to send system log messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which system log messages appear to come.
logging mail	Enables the security appliance to send system log messages by e-mail and determines which messages are sent by e-mail.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging savelog

To save the log buffer to Flash memory, use the **logging savelog** command in privileged EXEC mode.

logging savelog [*savefile*]

Syntax Description

savefile	(Optional) Saved Flash memory file name. If you do not specify the file name, the security appliance saves the log file using a default time-stamp format, as follows: `LOG-YYYY-MM-DD-HHMMSS.TXT` where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Defaults

The defaults are as follows:

- Buffer size is 4 KB.
- Minimum free Flash memory is 3 MB.
- Maximum Flash memory allocation for buffer logging is 1 MB.
- The default log file name is described in the “Syntax Description” section.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Before you can save the log buffer to Flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be saved to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

Note The **logging savelog** command does not clear the buffer. To clear the buffer, use the **clear logging buffer** command.

Examples

This example enables logging and the log buffer, exits global configuration mode, and saves the log buffer to Flash memory, using the file name latest-logfile.txt:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.

logging standby

To enable the failover standby security appliance to send the system log messages of this security appliance to logging destinations, use the **logging standby** command in global configuration mode. To disable system log messaging and SNMP logging, use the **no** form of this command.

logging standby

no logging standby

Syntax Description

This command has no arguments or keywords.

Defaults

The **logging standby** command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can enable **logging standby** to ensure that the system log messages of the failover standby security appliance stay synchronized if failover occurs.

Note Using the **logging standby** command causes twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

Examples

The following example enables the security appliance to send system log messages to the failover standby security appliance. The output of the **show logging** command reveals that this feature is enabled.

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
failover	Enables the failover feature.
logging enable	Enables logging.
logging host	Defines a syslog server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging timestamp

To specify that system log messages should include the date and time that the messages was generated, use the **logging timestamp** command in global configuration mode. To remove the date and time from system log messages, use the **no** form of this command.

logging timestamp

no logging timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

The security appliance does not include the date and time in system log messages by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging timestamp** command makes the security appliance include a timestamp in all system log messages.

Examples

The following example enables the inclusion of timestamp information in all system log messages:

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging trap

To specify which system log messages the security appliance sends to a syslog server, use the **logging trap** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

logging trap [*logging_list* | *level*]

no logging trap

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System unusable. • **1** or **alerts**—Take immediate action. • **2** or **critical**—Critical condition. • **3** or **errors**—Error. • **4** or **warnings**—Warning. • **5** or **notifications**—Normal but significant condition. • **6** or **informational**—Information. • **7** or **debugging**—Debug messages, log FTP commands, and WWW URLs.
logging_list	Specifies the list that identifies the messages to send to the syslog server. For information about creating lists, see the **logging list** command.

Defaults

No default system log message trap is defined.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you are using TCP as the logging transport protocol, the security appliance denies new network access sessions as a security measure if the security appliance is unable to reach the syslog server, if the syslog server is misconfigured, or if the disk is full.

UDP-based logging does not prevent the security appliance from passing traffic if the syslog server fails.

Examples

This example shows how to send system log messages of levels 0, 1, 2, and 3 to a syslog server that resides on the inside interface and uses the default protocol and port number.

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

login

To log into privileged EXEC mode using the local user database (see the username command) or to change user names, use the **login** command in user EXEC mode.

login

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

From user EXEC mode, you can log in to privileged EXEC mode as any username in the local database using the **login** command. The **login** command is similar to the **enable** command when you have enable authentication turned on (see the **aaa authentication console** command). Unlike enable authentication, the **login** command can only use the local username database, and authentication is always required with this command. You can also change users using the **login** command from any CLI mode.

To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the **aaa authorization command** for more information.

Caution If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

Examples

The following example shows the prompt after you enter the **login** command:

```
hostname> login
```

```
Username:
```

Related Commands

Command	Description
aaa authorization command	Enables command authorization for CLI access.
aaa authentication console	Requires authentication for console, Telnet, HTTP, SSH, or **enable** command access.
logout	Logs out of the CLI.
username	Adds a user to the local database.

login-button

To customize the Login button of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **login-button** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login button text is “Login”.

The default login button style is:

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the Login button with the text "OK":

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

Related Commands

Command	Description
login-title	Customizes the title of the WebVPN page login box.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.

login-message

To customize the login message of the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **login-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login message is “Please enter your username and password”.

The default login message style is background-color:#CCCCCC;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the login message text is set to "username and password":

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

Related Commands

Command	Description
login-title	Customizes the title of the login box on the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page login.
password-prompt	Customizes the password prompt of the WebVPN page login.
group-prompt	Customizes the group prompt of the WebVPN page login.

login-title

To customize the title of the login box on the WebVPN page displayed to WebVPN users, use the **login-title** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login text is “Login”.

The default HTML style of the login title is background-color: #666666; color: white.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the login title style:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

Command	Description
login-message	Customizes the login message of the WebVPN login page.
username-prompt	Customizes the username prompt of the WebVPN login page.
password-prompt	Customizes the password prompt of the WebVPN login page.
group-prompt	Customizes the group prompt of the WebVPN login page.

logo

To customize the logo on the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **logo** command from webvpn customization mode. To remove a logo from the configuration and reset the default (the Cisco logo), use the **no** form of this command.

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

Syntax Description

file	Indicates you are supplying a file containing a logo.
none	Indicates that there is no logo. Sets a null value, thereby disallowing a logo. Prevents inheriting a logo.
path	The path of the filename. The possible paths are disk0:, disk1:, or flash:
value	Specifies the filename of the logo. Maximum length is 255 characters, with no spaces. File type must be JPG, PNG, or GIF, and must be less than 100 KB.

Defaults

The default logo is the Cisco logo.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

If the filename you specify does not exist, an error message displays. If you remove a logo file but the configuration still points to it, no logo displays.

The filename cannot contain spaces.

Examples

In the following example, the file cisco_logo.gif contains a custom logo:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Related Commands

Command	Description
title	Customizes the title of the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

logout

To exit from the CLI, use the **logout** command in user EXEC mode.

logout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logout** command lets you log out of the security appliance. You can use the **exit** or **quit** commands to go back to unprivileged mode.

Examples

The following example shows how to log out of the security appliance:

```
hostname> logout
```

Related Commands

Command	Description
login	Initiates the log-in prompt.
exit	Exits an access mode.
quit	Exits configuration or privileged mode.

logout-message

To customize the logout message of the WebVPN logout screen that is displayed to WebVPN users when they logout from WebVPN service, use the **logout-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default logout message text is “Goodbye”.

The default logout message style is background-color:#999999;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the logout message style:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
italic; font-weight: bold
```

Related Commands

Command	Description
logout-title	Customizes the logout title of the WebVPN page.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.

CHAPTER 20

mac address through multicast-routing Commands

mac address

To specify the virtual MAC addresses for the active and standby units, use the **mac address** command in failover group configuration mode. To restore the default virtual MAC addresses, use the **no** form of this command.

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

Syntax Description

phy_if	The physical name of the interface to set the MAC address.
active_mac	The virtual MAC address for the active unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
standby_mac	The virtual MAC address for the standby unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Defaults

The defaults are as follows:

- Active unit default MAC address: 00a0.c9*physical_port_number.failover_group_id*01.
- Standby unit default MAC address: 00a0.c9*physical_port_number.failover_group_id*02.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If the virtual MAC addresses are not defined for the failover group, the default values are used.

If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address.

Examples

The following partial example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
```

```
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover mac address	Specifies a virtual MAC address for a physical interface.

mac-address

To manually assign a private MAC address to an interface or subinterface, use the **mac-address** command in interface configuration mode. In multiple context mode, this command can assign a different MAC address to the interface in each context. To revert the MAC address to the default, use the **no** form of this command.

mac-address *mac_address* [**standby** *mac_address*]

no mac-address [*mac_address* [**standby** *mac_address*]]

Syntax Description

mac_address	Sets the MAC address for this interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. If you use failover, this MAC address is the active MAC address. **Note** Because auto-generated addresses (the **mac-address auto** command) start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.
standby *mac_address*	(Optional) Sets the standby MAC address for failover. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Defaults

The default MAC address is the burned-in MAC address of the physical interface. Subinterfaces inherit the physical interface MAC address. Some commands set the physical interface MAC address (including this command in single mode), so the inherited address depends on that configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(5)	The use of A2 to start the MAC address was restricted when also used with the **mac-address auto** command.

Usage Guidelines

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information.

You can assign each MAC address manually with this command, or you can automatically generate MAC addresses for shared interfaces in contexts using the **mac-address auto** command. If you automatically generate MAC addresses, you can use the **mac-address** command to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

You can also set the MAC address using other commands or methods. The MAC address methods have the following priority:

1. **mac-address** command in interface configuration mode.

   This command works for physical interfaces and subinterfaces. In multiple context mode, you set the MAC address within each context. This feature lets you set a different MAC address for the same interface in multiple contexts.

2. **failover mac address** command for Active/Standby failover in global configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

3. **mac address** command for Active/Active failover in failover group configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

4. **mac-address auto** command in global configuration mode (multiple context mode only).

   This command applies to shared interfaces in contexts.

5. For Active/Active failover, auto-generation of active and standby MAC addresses for physical interfaces.

   This method applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

6. Burned-in MAC address. This method applies to physical interfaces.

   Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

Examples

The following example configures the MAC address for GigabitEthernet 0/1.1:

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address auto	Auto-generates MAC addresses (active and standby) for shared interfaces in multiple context mode.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

mac-address auto

To automatically assign private MAC addresses to each context interface, use the **mac-address auto** command in global configuration mode. To disable automatic MAC addresses, use the **no** form of this command.

mac-address auto prefix *prefix*

no mac-address auto

Syntax Description

prefix *prefix*	Sets the prefix used as part of the MAC address. The *prefix* is a decimal value between 0 and 65535. This prefix is converted to a 4-digit hexadecimal number. The prefix ensures that each security appliance uses unique MAC addresses, so you can have multiple security appliances on a network segment, for example. See the "MAC Address Format" section for more information about how the prefix is used.

Defaults

Auto-generation is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(5)	The **prefix** keyword was added. The MAC address format was changed to use the prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.

Usage Guidelines

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each shared context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for information about classifying packets.

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the **mac-address** command to manually set the MAC address.

Default MAC Address

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

All auto-generated MAC addresses start with A2. The auto-generated MAC addresses are persistent across reloads.

Interaction with Manual MAC Addresses

If you manually assign a MAC address and also enable auto-generation, then the manually assigned MAC address is used. If you later remove the manual MAC address, the auto-generated address is used.

Because auto-generated addresses start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.

Failover MAC Addresses

For use with failover, the security appliance generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption. See the "MAC Address Format" section for more information.

For upgrading failover units with the legacy version of the **mac-address auto** command before the **prefix** keyword was introduced, see the "Legacy MAC Address Format When Not Using the prefix Keyword" section.

MAC Address Format

The security appliance generates the MAC address using the following format:

A2xx.yyzz.zzzz

Where xx.yy is a user-defined prefix, and zz.zzzz is an internal counter generated by the security appliance. For the standby MAC address, the address is identical except that the internal counter is increased by 1.

For an example of how the prefix is used, if you set a prefix of 77, then the security appliance converts 77 into the hexadecimal value 004D (yyxx). When used in the MAC address, the prefix is reversed (xxyy) to match the security appliance native form:

A2**4D.00**zz.zzzz

For a prefix of 1009 (03F1), the MAC address is:

A2**F1.03**zz.zzzz

When the MAC Address is Generated

When you configure a **nameif** command for the interface in a context, the new MAC address is generated immediately. If you enable this command after you configure context interfaces, then MAC addresses are generated for all interfaces immediately after you enter the command. If you use the **no mac-address auto** command, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

Setting the MAC Address Uisng Other Methods

You can also set the MAC address using other commands or methods. The MAC address methods have the following priority:

1. **mac-address** command in interface configuration mode.

   This command works for physical interfaces and subinterfaces. In multiple context mode, you set the MAC address within each context. This feature lets you set a different MAC address for the same interface in multiple contexts.

2. **failover mac address** command for Active/Standby failover in global configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

3. **mac address** command for Active/Active failover in failover group configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

4. **mac-address auto** command in global configuration mode (multiple context mode only).

   This command applies to shared interfaces in contexts.

5. For Active/Active failover, auto-generation of active and standby MAC addresses for physical interfaces.

   This method applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

6. Burned-in MAC address. This method applies to physical interfaces.

   Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

Viewing MAC Addresses in the System Configuration

To view the assigned MAC addresses from the system execution space, enter the **show running-config all context** command.

The **all** option is required to view the assigned MAC addresses. Although this command is user-configurable in global configuration mode only, the **mac-address auto** command appears as a read-only entry in the configuration for each context along with the assigned MAC address. Only allocated interfaces that are configured with a **nameif** command within the context have a MAC address assigned.

Note If you manually assign a MAC address to an interface, but also have auto-generation enabled, the auto-generated address continues to show in the configuration even though the manual MAC address is the one that is in use. If you later remove the manual MAC address, the auto-generated one shown will be used.

Viewing MAC Addresses Within a Context

To view the MAC address in use by each interface within the context, enter the **show interface | include (Interface)|(MAC)** command.

Note The **show interface** command shows the MAC address in use; if you manually assign a MAC address and also have auto-generation enabled, then you can only view the unused auto-generated address from within the system configuration.

Legacy MAC Address Format When Not Using the prefix Keyword

Prior to Version 8.0(5), the **mac-address auto** command did not include the **prefix** keyword. This old version of the command is still accepted so you can perform upgrades between failover pairs; the command is not automatically converted when you upgrade so the commands continue to match between the upgraded and non-upgraded failover units. After you upgrade both units to the new software version, you should change this command to use the **prefix** keyword.

Without the **prefix** keyword, the MAC address is generated using the following format:

- Active unit MAC address: 12*_slot.port_subid.contextid*.
- Standby unit MAC address: 02*_slot.port_subid.contextid*.

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context, viewable with the **show context detail** command. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

- Active: 1200.0131.0001
- Standby: 0200.0131.0001

This legacy MAC address generation method does not allow for persistent MAC addresses across reloads, does not allow for multiple security appliances on the same network segment (because unique MAC addresses are not guaranteed), and does not prevent overlapping MAC addresses with manually assigned MAC addresses.

Examples

The following example enables automatic MAC address generation with a prefix of 78:

```
hostname(config)# mac-address auto prefix 78
```

The following output from the **show running-config all context admin** command shows the primary and standby MAC address assigned to the Management0/0 interface:

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

The following output from the **show running-config all context** command shows all the MAC addresses (primary and standby) for all context interfaces. Note that because the GigabitEthernet0/0 and GigabitEthernet0/1 main interfaces are not configured with a **nameif** command inside the contexts, no MAC addresses have been generated for them.

```
hostname# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
```

```
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address	Manually sets the MAC address (active and standby) for a physical interface or subinterface. In multiple context mode, you can set different MAC addresses in each context for the same interface.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

mac-address-table aging-time

To set the timeout for MAC address table entries, use the **mac-address-table aging-time** command in global configuration mode. To restore the default value of 5 minutes, use the **no** form of this command.

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

Syntax Description

timeout_value	The time a MAC address entry stays in the MAC address table before timing out, between 5 and 720 minutes (12 hours). 5 minutes is the default.

Defaults

The default timeout is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

No usage guidelines.

Examples

The following example sets the MAC address timeout to 10 minutes:

```
hostname(config)# mac-address-timeout aging time 10
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

mac-address-table static

To add a static entry to the MAC address table, use the **mac-address-table static** command in global configuration mode. To remove a static entry, use the **no** form of this command. Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the security appliance drops the traffic and generates a system message.

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

Syntax Description

interface_name	The source interface.
mac_address	The MAC address you want to add to the table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example adds a static MAC address entry to the MAC address table:

```
hostname(config)# mac-address-table static inside 0010.7cbe.6101
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.

Command	Description
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

mac-learn

To disable MAC address learning for an interface, use the **mac-learn** command in global configuration mode. To reenable MAC address learning, use the **no** form of this command. By default, each interface automatically learns the MAC addresses of entering traffic, and the security appliance adds corresponding entries to the MAC address table. You can disable MAC address learning if desired.

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

Syntax Description

interface_name	The interface on which you want to disable MAC learning.
disable	Disables MAC learning.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example disables MAC learning on the outside interface:

```
hostname(config)# mac-learn outside disable
```

Related Commands

Command	Description
clear configure mac-learn	Sets the **mac-learn** configuration to the default.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.
show running-config mac-learn	Shows the **mac-learn** configuration.

mac-list

To specify a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization, use the **mac-list** command in global configuration mode. To remove a MAC list entry, use the **no** form of this command.

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

Syntax Description

deny	Indicates that traffic matching this MAC address does not match the MAC list and is subject to both authentication and authorization when specified in the **aaa mac-exempt** command. You might need to add a deny entry to the MAC list if you permit a range of MAC addresses using a MAC address mask such as ffff.ffff.0000, and you want to force a MAC address in that range to be authenticated and authorized.
id	Specifies a hexadecimal MAC access list number. To group a set of MAC addresses, enter the **mac-list** command as many times as needed with the same ID value. The order of entries matters, because the packet uses the first entry it matches, as opposed to a best match scenario. If you have a permit entry, and you want to deny an address that is allowed by the permit entry, be sure to enter the deny entry before the permit entry.
mac	Specifies the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn
macmask	Specifies the portion of the MAC address that should be used for matching. For example, ffff.ffff.ffff matches the MAC address exactly. ffff.ffff.0000 matches only the first 8 digits.
permit	Indicates that traffic matching this MAC address matches the MAC list and is exempt from both authentication and authorization when specified in the **aaa mac-exempt** command.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To enable MAC address exemption from authentication and authorization, use the **aaa mac-exempt** command. You can only add one instance of the **aaa mac-exempt** command, so be sure that your MAC list includes all the MAC addresses you want to exempt. You can create multiple MAC lists, but you can only use one at a time.

Examples

The following example bypasses authentication for a single MAC address:

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2. Enter the deny statement before the permit statement, because 00a0.c95d.02b2 matches the permit statement as well, and if it is first, the deny statement will never be matched.

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
clear configure mac-list	Removes a list of MAC addresses previously specified by the **mac-list** command.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.

mail-relay

To configure a local domain name, use the **mail-relay** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

Syntax Description

domain_name	Specifies the domain name.
drop-connection	Closes the connection.
log	Generates a system log message.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a mail relay for a specific domain:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mail-relay mail action drop-connection
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

management-access

To allow management access to an interface other than the one from which you entered the security appliance when using VPN, use the **management-access** command in global configuration mode. To disable management access, use the **no** form of this command.

management-access *mgmt_if*

no management-access *mgmt_if*

Syntax Description

mgmt_if	Specifies the name of the management interface you want to access when entering the security appliance from another interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command allows you to connect to an interface other than the one you entered the security appliance from when using a full tunnel IPSec VPN or SSL VPN client (AnyConnect 2.x client, SVC 1.x) or across a site-to-site IPSec tunnel. For example, if you enter the security appliance from the outside interface, this command lets you connect to the inside interface using Telnet; or you can ping the inside interface when entering from the outside interface.

You can use the following applications:

- SNMP polls
- HTTPS requests
- ASDM access
- Telnet access
- SSH access
- PING
- Syslog polls
- NTP requests

You can define only one management-access interface.

Note Do not apply a static NAT statement to the management access interface; if you do so, then remote VPN users will not be able to access the management interface.

Examples

The following example shows how to configure a firewall interface named “inside” as the management access interface:

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the security appliance.
show management-access	Displays the name of the internal interface configured for management access.

Usage Guidelines

management-only

To set an interface to accept management traffic only, use the **management-only** command in interface configuration mode. To allow through traffic, use the **no** form of this command.

management-only

no management-only

Syntax Description

This command has no arguments or keywords.

Defaults

The Management 0/0 interface on the ASA 5510 and higher adaptive security appliance is set to management-only mode by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliance, you can use the Management 0/0 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only. You can also set the IP address of this interface in transparent mode if you want this interface to be on a different subnet from the management IP address, which is assigned to the security appliance or context, and not to individual interfaces.

Examples

The following example disables management-only mode on the management interface:

```
hostname(config)# interface management0/0
hostname(config-if)# no management-only
```

The following example enables management-only mode on a subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# management-only
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

map-name

To map a user-defined attribute name to a Cisco attribute name, use the **map-name** command in ldap-attribute-map configuration mode.

To remove this mapping, use the **no** form of this command.

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

Syntax Description

user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute.
Cisco-attribute-name	Specifies the Cisco attribute name that you are mapping to the user-defined name.

Defaults

By default, no name mappings exist.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
ldap-attribute-map configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **map-name** command, you can create map yourown attribute names to Cisco attribute names. You can then bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example commands map a user-defined attribute name Hours to the Cisco attribute name cVPN3000-Access-Hours in the LDAP attribute map myldapmap:

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
hostname(config-ldap-attribute-map)#
```

Within ldap-attribute-map mode, you can enter "?" to display the complete list of Cisco LDAP attribute names, as shown in the following example:

```
hostname(config-ldap-attribute-map)# map-name ?
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

map-value

To map a user-defined value to a Cisco LDAP attribute, use the **map-value** command in ldap-attribute-map configuration mode. To delete an entry within a map, use the **no** form of this command.

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

Syntax Description

cisco-value-string	Specifies the Cisco value string for the Cisco attribute.
user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute name.
user-value-string	Specifies the user-defined value string that you are mapping to the Cisco attribute value.

Defaults

By default, there are no user-defined values mapped to Cisco attributes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
ldap-attribute-map configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **map-value** command, you can map your own attribute values to Cisco attribute names and values. You can tthen bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example, entered in ldap-attribute-map mode, sets the user-defined value of the user attribute Hours to a user-defined time policy named workDay and a Cisco-defined time policy named Daytime:

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-value Hours workDay Daytime
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP maps.

mask

When using the Modular Policy Framework, mask out part of the packet that matches a **match** command or class map by using the **mask** command in match or class configuration mode. This mask action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. For example, you can you use **mask** command for the DNS application inspection to mask a header flag before allowing the traffic through the security appliance. To disable this action, use the **no** form of this command.

mask [**log**]

no mask [**log**]

Syntax Description

log	Logs the match. The system log message number depends on the application.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **mask** command to mask part of the packet that matches the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

Examples

The following example masks the RD and RA flags in the DNS header before allowing the traffic through the security appliance:

```
hostname(config-cmap)# policy-map type inspect dns dns-map1
```

```
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log
hostname(config-pmap-c)# match header-flag RA
hostname(config-pmap-c)# mask log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

mask-banner

To obfuscate the server banner, use the **mask-banner** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mask-banner

no mask-banner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to mask the server banner:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

mask-syst-reply

To hide the FTP server response from clients, use the **mask-syst-reply** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the **no** form of this command.

mask-syst-reply

no mask-syst-reply

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
FTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the mask-syst-reply command with strict FTP inspection to protect the FTP server system from clients. After enabling this command, the servers replies to the **syst** command are replaced by a series of Xs.

Examples

The following example causes the security appliance to replace the FTP server replies to the syst command with Xs:

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-map)#
```

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.

Commands	Description
policy-map	Associates a class map with specific security actions.
request-command deny	Specifies FTP commands to disallow.

match access-list

When using the Modular Policy Framework, use an access list to identify traffic to which you want to apply actions by using the **match access-list** command in class-map configuration mode. To remove the **match access-list** command, use the **no** form of this command.

match access-list *access_list_name*

no match access-list *access_list_name*

Syntax Description

access_list_name	Specifies the name of an access list to be used as match criteria.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

   After you enter the **class-map** command, you can enter the **match access-list** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You can only include one **match access-list** command in the class map, and you cannot combine it with other types of **match** commands. The exception is if you define the **match default-inspection-traffic** command which matches the default TCP and UDP ports used by all applications that the security appliance can inspect, then you can narrow the traffic to match using a **match access-list** command. Because the **match default-inspection-traffic** command specifies the ports to match, any ports in the access list are ignored.

2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

The following example creates three Layer 3/4 class maps that match three access lists:

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match any

When using the Modular Policy Framework, match all traffic to which you want to apply actions by using the **match any** command in class-map configuration mode. To remove the **match any** command, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

   After you enter the **class-map** command, you can enter the **match any** command to identify all traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You cannot combine the **match any** command with other types of **match** commands.

2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

This example shows how to define a traffic class using a class map and the **match any** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match any
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match apn

To configure a match condition for an access point name in GTP messages, use the **match apn** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP class map or policy map. Only one entry can be entered in a GTP class map.

Examples

The following example shows how to configure a match condition for an access point name in an GTP inspection class map:

```
hostname(config-cmap)# match apn class gtp_regex_apn
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match body

To configure a match condition on the length or length of a line of an ESMTP body message, use the **match body** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **body [length | line length] gt** *bytes*

no match [**not**] **body [length | line length] gt** *bytes*

Syntax Description

length	Specifies the length of an ESMTP body message.
line length	Specifies the length of a line of an ESMTP body message.
bytes	Specifies the number to match in bytes.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for a body line length in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match body line length gt 1000
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match called-party

To configure a match condition on the H.323 called party, use the **match called-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **called-party [regex** *regex***]**

no match [**not**] **match** [**not**] **called-party [regex** *regex***]**

Syntax Description

regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the called party in an H.323 inspection class map:

```
hostname(config-cmap)# match called-party regex caller1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match calling-party

To configure a match condition on the H.323 calling party, use the **match calling-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **calling-party [regex** *regex***]**

no match [**not**] **match** [**not**] **calling-party [regex** *regex***]**

Syntax Description

regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the calling party in an H.323 inspection class map:

```
hostname(config-cmap)# match calling-party regex caller1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match certificate

During the PKI certificate validation process, the security appliance checks certificate revocation status to maintain security. It can use either CRL checking or Online Certificate Status Protocol (OCSP) to accomplish this task. With CRL checking, the security appliance retrieves, parses, and caches Certificate Revocation Lists, which provide a complete list of revoked certificates. OCSP offers a more scalable method of checking revocation status in that it localizes certificate status on a Validation Authority, which it queries for the status of a specific certificate.

Certificate match rules let you configure OCSP URL overrides, which specify a URL to check for revocation status, rather than the URL in the AIA field of the remote user certificate. Match rules also let you configure trustpoints to use to validate OCSP responder certificates, which lets the security appliance validate responder certificates from any CA, including self-signed certificates and certificates external to the validation path of the client certificate.

To configure a certificate match rule, use the **match certificate** command in crypto ca trustpoint mode. To remove the rule from the configuration, use the **no** form of this command.

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

Syntax Description

map-name	Specifies the name of the certificate map to match to this rule. You must configure the certificate map prior to configuring a match rule. Maximum 65 characters.
match certificate	Specifies the certificate map for this match rule.
override ocsp	Specifies that the purpose of the rule is to override an OCSP URL in a certificate.
seq-num	Sets the priority for this match rule. Range is 1 to 10000. The security appliance evaluates the match rule with the lowest sequence number first, followed by higher numbers until it finds a match.
trustpoint	(Optional) Specifies using a trustpoint for verifying the OCSP responder certificate.
trustpoint-name	(Optional) Identifies the trustpoint. to use with the override to validate responder certificates.
url	Specifies accessing a URL for OCSP revocation status.
URL	Identifies the URL to access for OCSP revocation status.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
crypto ca trustpoint mode	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Be aware of the following tips when configuring OCSP:

- You can configure multiple match rules within a trustpoint configuration, but you can have only one match rule for each crypto ca certificate map. You can, however, configure multiple crypto ca certificate maps and associate them with the same trustpoint.
- You must configure the certificate map before configuring a match rule.
- To configure a trustpoint to validate a self-signed OCSP responder certificates, you import the self-signed responder certificate into its own trustpoint as a trusted CA certificate. Then you configure the **match certificate** command in the client certificate validating trustpoint to use the trustpoint that contains the self-signed OCSP responder certificate to validate the responder certificate. The same applies for validating responder certificates external to the validation path of the client certificate.
- A trustpoint can validate both the client certificate and the responder certificate if the same CA issues both of them. But if different CAs issue the client and responder certificates, you need to configure two trustpoints, one trustpoint for each certificate.
- The OCSP server (responder) certificate typically signs the OCSP response. After receiving the response, the security appliance tries to verify the responder certificate. The CA normally sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of it being compromised.The CA typically also includes an ocsp-no-check extension in the responder certificate indicating that this certificate does not need revocation status checking. But if this extension is not present, the security appliance tries to check its revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fails. To avoid this possibility, configure **revocation-check none** in the responder certificate validating trustpoint, while configuring r**evocation-check ocsp** for the client certificate.
- If the security appliance does not find a match, it uses the URL in the **ocsp url** command. If you have not configured the **ocsp url** command, it uses the AIA field of the remote user certificate. If the certificate does not have an AIA extension, revocation status checking fails.

Examples

The following example shows how to create a certificate match rule for a trustpoint called newtrust. The rule has a map name called mymap, sequence number of 4, a trustpoint called mytrust, and specifies a URL of 10.22.184.22.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
hostname(config-ca-trustpoint)#
```

The next example shows step-by-step how to configure a crypto ca certificate map, and then a match certificate rule to identify a trustpoint that contains a CA certificate to validate the responder certificate. This is necessary if the CA identified in the newtrust trustpoint does not issue an OCSP responder certificate.

Step 1 Configure the certificate map that identifies the client certificates to which the map rule applies. In this example the name of the certificate map is mymap and the sequence number is 1. Any client certificate with a subject-name that contains a CN attribute equal to mycert matches the mymap entry.

```
hostname(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
hostname(config-ca-cert-map)#
```

Step 2 Configure a trustpoint that contains the CA certificate to use to validate the OCSP responder certificate. In the case of self-signed certificates, this is the self-signed certificate itself, which is imported and locally trusted. You can also obtain a certificate for this purpose through external CA enrollment. When prompted to do so, paste in the CA certificate.

```
hostname(config-ca-cert-map)# exit
hostname(config)# crypto ca trustpoint mytrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Step 3 Configure the original trustpoint, newtrust, with OCSP as the revocation checking method. Then set a match rule that includes the certificate map, mymap, and the self-signed trustpoint, mytrust, configured in Step 2.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

Any connection that uses the newtrust trustpoint for client certificate authentication checks to see if the client certificate matches the attribute rules specified in the mymap certificate map. If so, the security appliance accesses the OCSP responder at 10.22.184.22 for certificate revocation status. It then uses the mytrust trustpoint to validate the responder certificate.

Note The newtrust trustpoint is configured to perform revocation checking via OCSP for the client certificates. However, the mytrust trustpoint is configured for the default revocation-check method which is none, so no revocation checking is performed on the OCSP responder certificate.

Related Commands

Command	Description
crypto ca certificate map	Creates crypto ca certificate maps. Use this command in global configuration mode.
crypto ca trustpoint	Enters crypto ca trustpoint mode. Use this command in global configuration mode.
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

match cmd

To configure a match condition on the ESMTP command verb, use the **match cmd** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **cmd [verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

no match [**not**] **cmd [verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

Syntax Description

verb *verb*	Specifies the ESMTP command verb.
line length gt *bytes*	Specifies the length of a line.
RCPT count gt *recipients_number*	Specifies the number of recipient email addresses.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition in an ESMTP inspection policy map for the verb (method) NOOP exchanged in the ESMTP transaction:

```
hostname(config-pmap)# match cmd verb NOOP
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match default-inspection-traffic

To specify default traffic for the inspect commands in a class map, use the **match default-inspection-traffic** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match default-inspection-traffic

no match default-inspection-traffic

Syntax Description

This command has no arguments or keywords.

Defaults

See the Usage Guidelines section for the default traffic of each inspection.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Using the **match default-inspection-traffic** command, you can match default traffic for the individual **inspect** commands. The **match default-inspection-traffic** command can be used in conjunction with one other match command, which is typically an access-list in the form of **permit ip** *src-ip dst-ip*.

The rule for combining a second **match** command with the **match default-inspection-traffic** command is to specify the protocol and port information using the **match default-inspection-traffic** command and specify all other information (such as IP addresses) using the second **match** command. Any protocol or port information specified in the second **match** command is ignored with respect to the **inspect** commands.

For instance, port 65535 specified in the example below is ignored:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# match port 65535
```

Default traffic for inspections are as follows:

Inspection Type	Protocol Type	Source Port	Destination Port
ctiqbe	tcp	N/A	1748
dcerpc	tcp	N/A	135
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
im	tcp	N/A	1-65539
ipsec-pass-thru	udp	N/A	500
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp,udp	N/A	5060
skinny	tcp	N/A	2000
smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

Examples

The following example shows how to define a traffic class using a class map and the **match default-inspection-traffic** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.

Command	Description
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match dns-class

To configure a match condition for the Domain System Class in a DNS Resource Record or Question section, use the **match dns-class** command in class-map or policy-map configuration mode. To remove a configured class, use the **no** form of this command.

match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

Syntax Description

eq	Specifies an exact match.
c_well_known	Specifies DNS class by well-known name, IN.
c_val	Specifies an arbitrary value in the DNS class field (0-65535).
range	Specifies a range.
c_val1 c_val2	Specifies values in a range match. Each value between 0 and 65535.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects all fields (questions and RRs) of a DNS message and matches the specified class. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: **match not header-flag QR** and **match question**.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS class in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-class eq IN
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match dns-type

To configure a match condition for a DNS type, including Query type and RR type, use the **match dns-type** command in class-map or policy-map configuration mode. To remove a configured dns type, use the **no** form of this command.

match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

Syntax Description

eq	Specifies an exact match.
t_well_known	Specifies DNS type by well-known name: A, NS, CNAME, SOA, TSIG, IXFR, or AXFR.
t_val	Specifies an arbitrary value in the DNS type field (0-65535).
range	Specifies a range.
t_val1 t_val2	Specifies values in a range match. Each value between 0 and 65535.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects all sections of a DNS message (questions and RRs) and matches the specified type. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: **match not header-flag QR** and **match question**.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS type in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
```

```
hostname(config-pmap)# match dns-type eq a
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match domain-name

To configure a match condition for a DNS message domain name list, use the **match domain-name** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **domain-name regex** *regex_id*

match [**not**] **domain-name regex class** *class_id*

no match [**not**] **domain-name regex** *regex_id*

no match [**not**] **domain-name regex class** *class_id*

Syntax Description

regex	Specifies a regular expression.
regex_id	Specifies the regular expression ID.
class	Specifies the class map that contains multiple regular expression entries.
class_id	Specifies the regular expression class map ID.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command matches domain names in the DNS message against predefined list. Compressed domain names will be expanded before matching. The match condition can be narrowed down to a particular field in conjunction with other DNS **match** commands.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to match the DNS domain name in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match domain-name regex
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match dscp

To identify the IETF-defined DSCP value (in an IP header) in a class map, use the **match dscp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match dscp {*values*}

no match dscp {*values*}

Syntax Description

values	Specifies up to eight different the IETF-defined DSCP values in the IP header. Range is 0 to 63.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Using the **match dscp** command, you can match the IETF-defined DSCP values in the IP header.

Examples

The following example shows how to define a traffic class using a class map and the **match dscp** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match dscp af43 cs1 ef
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match port	Specifies the TCP/UDP ports as the comparison criteria for packets received on that interface.
show running-config class-map	Displays the information about the class map configuration.

match ehlo-reply-parameter

To configure a match condition on the ESMTP ehlo reply parameter, use the **match ehlo-reply-parameter** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **ehlo-reply-parameter** *parameter*

no match [**not**] **ehlo-reply-parameter** *parameter*

Syntax Description

parameter	Specifies the ehlo reply parameter.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for an ehlo reply parameter in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match ehlo-reply-parameter auth
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match filename

To configure a match condition for a filename for FTP transfer, use the **match filename** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filename in an FTP inspection class map:

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
hostname(config-cmap)# match username regex class ftp_regex_user
hostname(config-cmap)# match filename regex ftp-file
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match filetype

To configure a match condition for a filetype for FTP transfer, use the **match filetype** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP transfer filetype in an FTP inspection policy map:

```
hostname(config-pmap)# match filetype class regex ftp-regex-filetype
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match flow ip destination-address

To specify the flow IP destination address in a class map, use the **match flow ip destination-address** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match flow ip destination-address

no match flow ip destination-address

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions on a tunnel group, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **match flow ip destination-address** command. Use **match tunnel-group** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for VPN.

match header

To configure a match condition on the ESMTP header, use the **match header** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

no match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

Syntax Description

length gt *bytes*	Specifies to match on the length of the ESMTP header message.
line length gt bytes	Specifies to match on the length of a line of an ESMTP header message.
to-fields count gt *to_fields_number*	Specifies to match on the number of To: fields.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for a header in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match header length gt 512
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match header-flag

To configure a match condition for a DNS header flag, use the **match header-flag** command in class-map or policy-map configuration mode. To remove a configured header flag, use the **no** form of this command.

match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

no match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

Syntax Description

eq	Specifies an exact match. If not configured, specifies a **match-all** bit mask match.
f_well_known	Specifies DNS header flag bits by well-known name. Multiple flag bits may be entered and logically OR'd. QR (Query, note: QR=1, indicating a DNS response) AA (Authoritative Answer) TC (TrunCation) RD (Recursion Desired) RA (Recursion Available)
f_value	Specifies an arbitrary 16-bit value in hexidecimal form.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a DNS class map or policy map. Only one entry can be entered in a DNS class map.

Examples

The following example shows how to configure a match condition for a DNS header flag in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match header-flag AA
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match im-subscriber

To configure a match condition for a SIP IM subscriber, use the **match im-subscriber** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for a SIP IM subscriber in a SIP inspection class map:

```
hostname(config-cmap)# match im-subscriber regex class im_sender
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match invalid-recipients

To configure a match condition on the ESMTP invalid recipient address, use the **match invalid-recipients** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **invalid-recipients count gt** *number*

no match [**not**] **invalid-recipients count gt** *number*

Syntax Description

count gt *number*	Specifies to match on the invalid recipient number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for invalid recipients count in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match invalid-recipients count gt 1000
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match ip address

To redistribute any routes that have a route address or match packet that is passed by one of the access lists specified, use the **match ip address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ip address {*acl...*}

no match ip address {*acl...*}

Syntax Description

acl	Name an access list. Multiple access lists can be specified.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

Examples

The following example shows how to redistribute internal routes:

```
hostname(config)# route-map name
hostname(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip next-hop

To redistribute any routes that have a next-hop router address that is passed by one of the access lists specified, use the **match ip next-hop** command in route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

no match ip next-hop {*acl...*} | **prefix-list** *prefix_list*

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix-list *prefix_list*	Name of prefix list.

Defaults

Routes are distributed freely, without being required to match a next-hop address.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *acl* argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows how to distribute routes that have a next-hop router address passed by access list acl_dmz1 or acl_dmz2:

```
hostname(config)# route-map name
hostname(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match ip route-source

To redistribute routes that have been advertised by routers and access servers at the address that is specified by the ACLs, use the **match ip route-source** command in the route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip route-source {*acl...*} | **prefix-list** *prefix_list*

no match ip route-source {*acl...*}

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
prefix_list	Name of prefix list.

Defaults

No filtering on a route source.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-name argument.

The **route-map global** configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match. The next-hop and source-router address of the route are not the same in some situations.

Examples

The following example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by ACLs acl_dmz1 and acl_dmz2:

```
hostname(config)# route-map name
hostname(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified.
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the ACLs specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match login-name

To configure a match condition for a client login name for instant messaging, use the **match login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for a client login name in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match login-name regex login
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match media-type

To configure a match condition on the H.323 media type, use the **match media-type** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **media-type [audio | data | video]**

no match [**not**] **media-type [audio | data | video]**

Syntax Description

audio	Specifies to match audio media type.
data	Specifies to match data media type.
video	Specifies to match video media type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for audio media type in an H.323 inspection class map:

```
hostname(config-cmap)# match media-type audio
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match message id

To configure a match condition for a GTP message ID, use the **match message id** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message id [***message_id* | **range** *lower_range upper_range*]

no match [**not**] **message id [***message_id* | **range** *lower_range upper_range*]

Syntax Description

message_id	Specifies an alphanumeric identifier between 1 and 255.
range *lower_range upper_range*	Specifies a lower and upper range of IDs.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP class map or policy map. Only one entry can be entered in a GTP class map.

Examples

The following example shows how to configure a match condition for a message ID in a GTP inspection class map:

```
hostname(config-cmap)# match message id 33
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match message length

To configure a match condition for a GTP message ID, use the **match message length** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **message length min** *min_length* **max** *max_length*

no match [**not**] **message length min** *min_length* **max** *max_length*

Syntax Description

min *min_length*	Specifies a minimum message ID length. Value is between 1 and 65536.
max *max_length*	Specifies a maximum message ID length. Value is between 1 and 65536.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP class map or policy map. Only one entry can be entered in a GTP class map.

Examples

The following example shows how to configure a match condition for a message length in a GTP inspection class map:

```
hostname(config-cmap)# match message length min 8 max 200
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match message-path

To configure a match condition for the path taken by a SIP message as specified in the Via header field, use the **match message-path** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
hostname(config-cmap)# match message-path regex class sip_message
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match mime

To configure a match condition on the ESMTP mime encoding type, mime filename length, or mime file type, use the **match mime** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

no match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

Syntax Description

encoding *type*	Specifies to match on the encoding type.
filename length gt *bytes*	Specifies to match on the filename length.
filetype *regex*	Specifies to match on the file type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for a mime filename length in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match mime filename length gt 255
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match peer-ip-address

To configure a match condition for the peer IP address for instant messaging, use the **match peer-ip-address** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-ip-address** *ip_address ip_address_mask*

no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

Syntax Description

ip_address	Specifies a hostname or IP address of the client or server.
ip_address_mask	Specifies the netmask for the client or server IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer IP address in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match peer-login-name

To configure a match condition for the peer login name for instant messaging, use the **match peer-login-name** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the peer login name in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-login-name regex peerlogin
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match port

When using the Modular Policy Framework, match the TCP or UDP ports to which you want to apply actions by using the **match port** command in class-map configuration mode. To remove the **match port** command, use the **no** form of this command.

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

Syntax Description

eq *port*	Specifies a single port name or number.
range *beg_port end_port*	Specifies beginning and ending port range values between 1 and 65535.
tcp	Specifies a TCP port.
udp	Specifies a UDP port.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.

   After you enter the **class-map** command, you can enter the **matchport** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** command (the **class-map type management** command only allows the match port command). You can only include one **match port** command in the class map, and you cannot combine it with other types of **match** commands.

2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

The following example shows how to define a traffic class using a class map and the **match port** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 8080
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match precedence

To specify a precedence value in a class map, use the **match precedence** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match precedence *value*

no match precedence *value*

Syntax Description

value	Specifies up to four precedence values separated by a space. Range is 0 to 7.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match precedence** command to specify the value represented by the TOS byte in the IP header.

Examples

The following example shows how to define a traffic class using a class map and the **match precedence** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match precedence 1
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match protocol

To configure a match condition for a specific instant messaging protocol, such as MSN or Yahoo, use the **match protocol** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **protocol** {**msn-im** | **yahoo-im**}

no match [**not**] **protocol** {**msn-im** | **yahoo-im**}

Syntax Description

msn-im	Specifies to match the MSN instant messaging protocol.
yahoo-im	Specifies to match the Yahoo instant messaging protocol.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the Yahoo instant messaging protocol in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match protocol yahoo-im
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match question

To configure a match condition for a DNS question or resource record, use the **match question** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match {**question** | {**resource-record answer** | **authority** | **additional**}}

no match {**question** | {**resource-record answer** | **authority** | **additional**}}

Syntax Description

question	Specifies the question portion of a DNS message.
resource-record	Specifies the resource record portion of a DNS message.
answer	Specifies the Answer RR section.
authority	Specifies the Authority RR section.
additional	Specifies the Additional RR section.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects the DNS header and matches the specified field. It can be used in conjunction with other DNS **match** commands to define inspection of a particular question or RR type..

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS question in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match question
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match req-resp

To configure a match condition for both HTTP requests and responses, use the **match req-resp** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **req-resp content-type mismatch**

no match [**not**] **req-resp content-type mismatch**

Syntax Description

content-type	Specifies to match the content type in the response to the accept types in the request.
mismatch	Specifies that the content type field in the response must match one of the mime types in the accept field of the request.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command enables the following checks:

- Verifies that the value of the header content-type is in the internal list of supported content types,
- Verifies that the header content-type matches the actual content in the data or entity body portion of the message.
- Verifies the content type field in the HTTP response matches the **accept** field in the corresponding HTTP request message.

If the message fails any of the above checks, the security appliance takes the configured action.

The following is the list of supported content types.

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

Some content-types in this list may not have a corresponding regular expression (magic number) so they cannot be verified in the body portion of the message. When this case occurs, the HTTP message will be allowed.

Examples

The following example shows how to restrict HTTP traffic based on the content type of the HTTP message in an HTTP policy map:

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# match req-resp content-type mismatch
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match request-command

To restrict specific FTP commands, use the **match request-command** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **request-command** *ftp_command* [*ftp_command...*]

no match [**not**] **request-command** *ftp_command* [*ftp_command...*]

Syntax Description

ftp_command	Specifies one or more FTP commands to restrict.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for a specific FTP command in an FTP inspection policy map:

```
hostname(config)# policy-map type inspect ftp ftp_map1
hostname(config-pmap)# match request-command stou
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match request-method

To configure a match condition for the SIP method type, use the **match request-method** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **request-method** *method_type*

no match [**not**] **request-method** *method_type*

Syntax Description

method_type	Specifies a method type according to RFC 3261 and supported extensions. Supported method types include: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
hostname(config-cmap)# match request-method ack
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match request method

To configure a match condition for HTTP requests, use the **match request method** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

no match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

Syntax Description

built-in-regex	Specifies the built-in regex for content type, method, or transfer encoding.
class *class_map name*	Specifies the name of the class map of regex type.
regex *regex_name*	Specifies the name of the regular expression configured using the **regex** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Table 20-1 Built-in Regex Values

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

Examples

The following example shows how to define an HTTP inspection policy map that will allow and log any HTTP connection that attempts to access "www\.xyz.com/.*\.asp" or "www\.xyz[0-9][0-9]\.com" with methods "GET" or "PUT." All other URL/Method combinations will be silently allowed:

```
hostname(config)# regex url1 "www\.xyz.com/.*\.asp
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"
hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit
hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit
hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit
hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match route-type

To redistribute routes of the specified type, use the **match route-type** command in route-map configuration mode. To remove the route type entry, use the **no** form of this command.

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

Syntax Description

local	Locally generated BGP routes.
internal	OSPF intra-area and interarea routes or EIGRP internal routes.
external	OSPF external routes or EIGRP external routes.
type-1	(Optional) Specifies the route type 1.
type-2	(Optional) Specifies the route type 2.
nssa-external	Specifies the external NSSA.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **route-map** global configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

For OSPF, the **external type-1** keywords match only type 1 external routes and the **external type-2** keywords match only type 2 external routes.

Examples

The following example shows how to redistribute internal routes:

```
hostname(config)# route-map name
hostname(config-route-map)# match route-type internal
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match rtp

To specify a UDP port range of even-number ports in a class map, use the **match rtp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match rtp *starting_port range*

no match rtp *starting_port range*

Syntax Description

starting_port	Specifies lower bound of even-number UDP destination port. Range is 2000-65535
range	Specifies range of RTP ports. Range is 0-16383.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match rtp** command to match RTP ports (even UDP port numbers between the *starting_port* and the *starting_port* plus the *range*).

Examples

The following example shows how to define a traffic class using a class map and the **match rtp** command:

```
hostname(config)# class-map cmap
```

```
hostname(config-cmap)# match rtp 20000 100
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match sender-address

To configure a match condition on the ESMTP sender e-mail address, use the **match sender-address** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **sender-address [length gt** *bytes* **|** **regex** *regex***]**

no match [**not**] **sender-address [length gt** *bytes* **|** **regex** *regex***]**

Syntax Description

length gt *bytes*	Specifies to match on the sender e-mail address length.
regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the sender email address of length greater than 320 characters in an ESMTP inspection policy map:

```
hostname(config-pmap)# match sender-address length gt 320
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match server

To configure a match condition for an FTP server, use the **match server** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP server in an FTP inspection policy map:

```
hostname(config-pmap)# match server class regex ftp-server
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match service

To configure a match condition for a specific instant messaging service, use the **match service** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

no match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

Syntax Description

chat	Specifies to match the instant messaging chat service.
file-transfer	Specifies to match the instant messaging file transfer service.
games	Specifies to match the instant messaging games service.
voice-chat	Specifies to match the instant messaging voice chat service.
webcam	Specifies to match the instant messaging webcam service.
conference	Specifies to match the instant messaging conference service.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the chat service in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match service chat
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match third-party-registration

To configure a match condition for the requester of a third-party registration, use the **match third-party-registration** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

The third-party registration match command is used to identify the user who can register others with a SIP registar or SIP proxy. It is identified by the From header field in the REGISTER message in the case of mismatching From and To values.

Examples

The following example shows how to configure a match condition for third-party registration in a SIP inspection class map:

```
hostname(config-cmap)# match third-party-registration regex class sip_regist
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match tunnel-group

To match traffic in a class map that belongs to a previously defined tunnel-group, use the **match tunnel-group** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match tunnel-group *name*

no match tunnel-group *name*

Syntax Description

name	Text for the tunnel group name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **police** command. Use **match tunnel-group** along with **match flow ip destination-address** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and L2TP,

match uri

To configure a match condition for the URI in the SIP headers, use the **match uri** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

no match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

Syntax Description

sip	Specifies a SIP URI.
tel	Specifies a TEL URI.
length gt *gt_bytes*	Specifies the maximum length of the URI. Value is between 0 and 65536.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the URI in the SIP message:

```
hostname(config-cmap)# match uri sip length gt
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match url-filter

To configure a match condition for URL filtering in an RTSP message, use the **match url-filter** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command can be configured in an RTSP class map or policy map.

Examples

The following example shows how to configure a match condition for URL filtering in an RTSP inspection policy map:

```
hostname(config)# regex badurl www.url1.com/rtsp.avi
hostname(config)# policy-map type inspect rtsp rtsp-map
hostname(config-pmap)# match url-filter regex badurl
hostname(config-pmap-p)# drop-connection
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match username

To configure a match condition for an FTP username, use the **match username** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP username in an FTP inspection class map:

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# match username regex class ftp_regex_user
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match version

To configure a match condition for a GTP message ID, use the **match message length** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

Syntax Description

vresion_id	Specifies a version between 0 and 255.
range *lower_range upper_range*	Specifies a lower and upper range of versions.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP class map or policy map. Only one entry can be entered in a GTP class map.

Examples

The following example shows how to configure a match condition for a message version in a GTP inspection class map:

```
hostname(config-cmap)# match version 1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

max-failed-attempts

To specify the number of failed attempts allowed for any given server in the server group before that server is deactivated, use the **max-failed-attempts** command in AAA-server group configuration mode. To remove this specification and revert to the default value, use the **no** form of this command:

max-failed-attempts *number*

no max-failed-attempts

Syntax Description

number	An integer in the range 1-5, specifying the number of failed connection attempts allowed for any given server in the server group specified in a prior **aaa-server** command.

Defaults

The default value of *number* is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
AAA-server group configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have configured the AAA server/group before issuing this command.

Examples

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 4
hostname(config-aaa-server-group)#
```

Related Commands

Command	Description
aaa-server *server-tag* **protocol** *protocol*	Enters AAA server group configuration mode so you can configure AAA server parameters that are group-specific and common to all hosts in the group.

clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

max-forwards-validation

To enable check on Max-forwards header field of 0, use the **max-forwards-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

no max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection of a violation occurs.
log	Specifies standalone or additional log in case of violation. It can be associated to any of the actions.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command counts the number of hops to destination, which cannot be 0 before reaching the destination.

Examples

The following example shows how to enable max forwards validation in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# max-forwards-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

max-header-length

To restrict HTTP traffic based on the HTTP header length, use the **max-header-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
request	Request message.
reset	Send a TCP reset message to client and server.
response	(Optional) Response message.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **max-header-length** command, the security appliance only allows messages having an HTTP header within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the security appliance to reset the TCP connection and optionally create a syslog entry.

Examples

The following example restricts HTTP requests to those with HTTP headers that do not exceed 100 bytes. If a header is too large, the security appliance resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

max-object-size

To set a maximum size for objects that the security appliance can cache for WebVPN sessions, use the max-object-size command in cache mode. To change the size, use the command again.

max-object-size *integer range*

Syntax Description

integer range	0 - 10000 KB

Defaults

1000 KB

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cache mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The Maximum object size must be larger than the minimum object size. The security appliance calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 4000 KB:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# max-object-size 4000
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
min-object-size	Defines the minimum sizze of an object to cache.

max-retry-attempts

To configure the number of times the security appliance retries a failed SSO authentication attempt before letting the request time out, use the **max-retry-attempts** command in the webvpn configuration mode for the specific SSO server type.

To return to the default value, use the **no** form of this command.

max-retry-attempts *retries*

no max-retry-attempts

Syntax Description

retries	The number of times the security appliance retries a failed SSO authentication attempt. The range is 1 to 5 retries.

Defaults

The default value for this command is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

Once you have configured the security appliance to support SSO authentication, optionally you can adjust two timeout parameters:

- The number of times the security appliance retries a failed SSO authentication attempt using the **max-retry-attempts** command.
- The number of seconds before a failed SSO authentication attempt times out (see the **request-timeout** command).

Examples

The following example, entered in webvpn-sso-siteminder configuration mode, configures four authentication retries for the SiteMinder SSO server named my-sso-server:

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

max-uri-length

To restrict HTTP traffic based on the length of the URI in the HTTP request message, use the **max-uri-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
reset	Send a TCP reset message to client and server.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **max-uri-length** command, the security appliance only allows messages having a URI within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the security appliance to reset the TCP connection and create a syslog entry.

URIs with a length less than or equal to the configured value will be allowed. Otherwise, the specified action will be taken.

Examples

The following example restricts HTTP requests to those with URIs that do not exceed 100 bytes. If a URI is too large, the security appliance resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

mcc

To identify the mobile country code and the mobile network code for IMSI prefix filtering, use the **mcc** command in GTP map configuration mode. To remove the configuration, use the **no** form of this command.

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

Syntax Description

country_code	A non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
network_code	A two or three-digit value identifying the network code.

Defaults

By default, the security appliance does not check for valid MCC/MNC combinations.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used for IMSI Prefix filtering. The MCC and MNC in the IMSI of the received packet is compared with the MCC/MNC configured with this command and is dropped if it does not match.

This command must be used to enable IMSI Prefix filtering. You can configure multiple instances to specify permitted MCC and MNC combinations. By default, the security appliance does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Examples

The following example identifies traffic for IMSI Prefix filtering with an MCC of 111 and an MNC of 222:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
hostname(config-gtpmap)#
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

media-termination address

To specify the IP address to use for media connections to the Phone Proxy feature, use the **media-termination address** command in phone-proxy configuration mode.

To remove the media-termination address from the Phone Proxy configuration, use the **no** form of this command.

media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

no media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

Syntax Description

ip_address	Specifies the virtual IP address that will be created for the phone proxy to use during media termination. Only one virtual interface can be configured per phone-proxy instance. The ASA phone proxy inserts the media termination IP address into the media address portion of the signaling messages.
rtp-max-port *port2*	Specifies the maximum value for the RTP port range for the media termination point, where *port2* can be a value from 32767 to 65535.
rtp-min-port *port1*	Specifies the minimum value for the RTP port range for the media termination point, where *port1* can be a value from 1024 to 16384.

Defaults

By default, the *port1* value for the **rtp-min-port** keyword is 16384 and the *port2* value for the **rtp-max-port** keyword is 32767.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The security appliance must have an IP address for media termination that meets the following criteria:

- The IP address is a publicly routable address that is an unused IP address on an attached network to the security appliance interface that will never be used by another device in your network.
- The IP address cannot be the same as the security appliance interface IP address. Specifically, it cannot be the same as the least secure interface on the security appliance.
- The IP address cannot overlap with existing static NAT rules.
- The IP address cannot be the same as the CUCM or TFTP server IP address.

- Add routes to the other interfaces so that IP phones on other interfaces can reach the media termination address.

Configure the RTP port range for the media termination point when you need to scale the number of calls that the Phone Proxy supports.

Examples

The following example shows the use of the **media-termination address** command to specify the IP address to use for media connections:

```
hostname(config-phone-proxy)# media-termination address 192.168.1.4
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

media-type

To set the media type to copper or fiber Gigabit Ethernet, use the **media-type** command in interface configuration mode. The fiber SFP connector is available on the 4GE SSM for the ASA 5500 series adaptive security appliance. To restore the media type setting to the default, use the **no** form of this command.

media-type {**rj45** | **sfp**}

no media-type [rj45 | **sfp**]

Syntax Description

rj45	(Default) Sets the media type to the copper RJ-45 connector.
sfp	Sets the media type to the fiber SFP connector.

Defaults

The default is **rj45**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **sfp** setting uses a fixed speed (1000 Mbps), so the **speed** command allows you to set whether the interface negotiates link parameters or not. The **duplex** command is not supported for **sfp**.

Examples

The following example sets the media type to SFP:

```
hostname(config)# interface gigabitethernet1/1
hostname(config-if)# media-type sfp
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

member

To assign a context to a resource class, use the **member** command in context configuration mode. To remove the context from the class, use the **no** form of this command.

member *class_name*

no member *class_name*

Syntax Description

class_name	Specifies the class name you created with the **class** command.

Defaults

By default, the context is assigned to the default class.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the security appliance, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context. The security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

Examples

The following example assigns the context test to the gold class:

```
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
limit-resource	Sets the limit for a resource.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

member-interface

To assign a physical interface to a redundant interface, use the **member-interface** command in interface configuration mode. This command is available only for the redundant interface type. You can assign two member interfaces to a redundant interface. To remove a member interface, use the **no** form of this command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.

member-interface *physical_interface*

no member-interface *physical_interface*

Syntax Description

physical_interface	Identifies the interface ID, such as **gigabitethernet 0/1**. See the **interface** command for accepted values. Both member interfaces must be the same physical type.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Both member interfaces must be of the same physical type. For example, both must be Ethernet.

You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.

Caution If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters such as **speed** and **duplex** commands, the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.

If you shut down the active interface, then the standby interface becomes active.

To change the active interface, enter the **redundant-interface** command.

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the **mac-address** command or the **mac-address auto** command). When the active interface fails over to the standby, the same MAC address is maintained so traffic is not disrupted.

Examples

The following example creates two redundant interfaces:

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
redundant-interface	Changes the active member interface.
show interface	Displays the runtime status and statistics of interfaces.

memberof

To specify a list of group-names that this user is a member of, use the **memberof** command in username attributes configuration mode. To remove this attribute from the configuration, use the **no** form of this command.

memberof *group_1*[,*group_2*,...*group_n*]

[**no**] **memberof** *group_1*[,*group_2*,...*group_n*]

Syntax Description

group_1 through group_n	Specifies the groups to which this user belongs.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Username attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Enter a comma separated list of group names to which this user belongs.

Examples

The following example entered in global configuration mode, creates a username called newuser, then specifies that newuser is a member of the DevTest and management groups.

```
hostname(config)# username newuser nopassword
hostname(config)# username newuser attributes
hostname(config-username)# memberof DevTest,management
hostname(config-username)#
```

Related Commands

Command	Description
clear configure username	Clears the entire username database or just the specified username.
show running-config username	Displays the currently running username configuration for a specified user or for all users.
username	Creates and manages the database of user names.

memory delayed-free-poisoner enable

To enable the delayed free-memory poisoner tool, use the **memory delayed-free-poisoner enable** command in privileged EXEC mode. To disable the delayed free-memory poisoner tool, use the **no** form of this command. The delayed free-memory poisoner tool lets you monitor freed memory for changes after it has been released by an application.

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

Syntax Description

This command has no arguments or keywords.

Defaults

The **memory delayed-free-poisoner enable** command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enabling the delayed free-memory poisoner tool has a significant impact on memory usage and system performance. The command should only be used under the supervision of the Cisco TAC. It should not be run in a production environment during heavy system usage.

When you enable this tool, requests to free memory by the applications running on the security appliance are written to a FIFO queue. As each request is written to the queue, each associated byte of memory that is not required by lower-level memory management is “poisoned” by being written with the value 0xcc.

The freed memory requests remain in the queue until more memory is required by an application than is in the free memory pool. When memory is needed, the first freed memory request is pulled from the queue and the poisoned memory is validated.

If the memory is unmodified, it is returned to the lower-level memory pool and the tool reissues the memory request from the application that made the initial request. The process continues until enough memory for the requesting application is freed.

If the poisoned memory has been modified, then the system forces a crash and produces diagnostic output to determine the cause of the crash.

The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically. Validation can also be started manually using the **memory delayed-free-poisoner validate** command.

The **no** form of the command causes all of the memory referenced by the requests in the queue to be returned to the free memory pool without validation and any statistical counters to be cleared.

Examples

The following example enables the delayed free-memory poisoner tool:

```
hostname# memory delayed-free-poisoner enable
```

The following is sample output when the delayed free-memory poisoner tool detects illegal memory reuse:

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |           ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

Table 20-2 describes the significant portion of the output.

Table 20-2 Illegal Memory Usage Output Description

Field	Description
heap region	The address region and size of the region of memory available for use by the requesting application. This is not the same as the requested size, which may be smaller given the manner in which the system may parcel out memory at the time the memory request was made.
memory address	The location in memory where the fault was detected.
byte offset	The byte offset is relative to the beginning of the heap region and can be used to find the field that was modified if the result was used to hold a data structure starting at this address. A value of 0 or that is larger than the heap region byte count may indicate that the problem is an unexpected value in the lower level heap package.

Table 20-2 Illegal Memory Usage Output Description

Field	Description
allocated by/freed by	Instruction addresses where the last malloc/calloc/realloc and free calls where made involving this particular region of memory.
Dumping...	A dump of one or two regions of memory, depending upon how close the detected fault was to the beginning of the region of heap memory. The next eight bytes after any system heap header is the memory used by this tool to hold a hash of various system header values plus the queue linkage. All other bytes in the region until any system heap trailer is encountered should be set to 0xcc.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory delayed-free-poisoner validate

To force validation of all elements in the **memory delayed-free-poisoner** queue, use the **memory delayed-free-poisoner validate** command in privileged EXEC mode.

memory delayed-free-poisoner validate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must enable the delayed free-memory poisoner tool using the **memory delayed-free-poisoner enable** command before issuing the **memory delayed-free-poisoner validate** command.

The **memory delayed-free-poisoner validate** command causes each element of the **memory delayed-free-poisoner** queue to be validated. If an element contains unexpected values, then the system forces a crash and produces diagnostic output to determine the cause of the crash. If no unexpected values are encountered, the elements remain in the queue and are processed normally by the tool; the **memory delayed-free-poisoner validate** command does not cause the memory in the queue to be returned to the system memory pool.

Note The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically.

Examples

The following example causes all elements in the **memory delayed-free-poisoner** queue to be validated:

```
hostname# memory delayed-free-poisoner validate
```

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory caller-address

To configure a specific range of program memory for the call tracing, or caller PC, to help isolate memory problems, use the **memory caller-address** command in privileged EXEC mode. The caller PC is the address of the program that called a memory allocation primitive. To remove an address range, use the **no** form of this command.

memory caller-address *startPC endPC*

no memory caller-address

Syntax Description

endPC	Specifies the end address range of the memory block.
startPC	Specifies the start address range of the memory block.

Defaults

The actual caller PC is recorded for memory tracing.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **memory caller-address** command to isolate memory problems to a specific block of memory.

In certain cases the actual caller PC of the memory allocation primitive is a known library function that is used at many places in the program. To isolate individual places in the program, configure the start and end program address of the library function, thereby recording the program address of the caller of the library function.

Note The security appliance might experience a temporary reduction in performance when caller-address tracing is enabled.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464
```

```
hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory-caller address	Displays the address ranges configured on the security appliance.

memory profile enable

To enable the monitoring of memory usage (memory profiling), use the **memory profile enable** command in privileged EXEC mode. To disable memory profiling, use the **no** form of this command.

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

Syntax Description

peak_value	Specifies the memory usage threshold at which a snapshot of the memory usage is saved to the peak usage buffer. The contents of this buffer could be analyzed at a later time to determine the peak memory needs of the system.

Defaults

Memory profiling is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Before enabling memory profiling, you must first configure a memory text range to profile with the **memory profile text** command.

Some memory is held by the profiling system until you enter the **clear memory profile** command. See the output of the **show memory status** command.

Note The security appliance might experience a temporary reduction in performance when memory profiling is enabled.

The following example enables memory profiling:

```
hostname# memory profile enable
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.

memory profile text

To configure a program text range of memory to profile, use the **memory profile text** command in privileged EXEC mode. To disable, use the **no** form of this command.

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

Syntax Description

all	Specifies the entire text range of the memory block.
endPC	Specifies the end text range of the memory block.
resolution	Specifies the resolution of tracing for the source text region.
startPC	Specifies the start text range of the memory block.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

For a small text range, a resolution of "4" normally traces the call to an instruction. For a larger text range, a coarse resolution is probably enough for the first pass and the range could be narrowed down to a set of smaller regions in the next pass.

After entering the text range with the **memory profile text** command, you must then enter the **memory profile enable** command to begin memory profiling. Memory profiling is disabled by default.

Note The security appliance might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows how to configure a text range of memory to profile, with a resolution of 4:

```
hostname# memory profile text 0x004018b4 0x004169d0 4
```

The following example displays the configuration of the text range and the status of memory profiling (OFF):

```
hostname# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

Note To begin memory profiling, you must enter the **memory profile enable** command. Memory profiling is disabled by default.

Related Commands

Command	Description
clear memory profile	Clears the buffers held by the memory profiling function.
memory profile enable	Enables the monitoring of memory usage (memory profiling).
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory-caller address	Displays the address ranges configured on the security appliance.

memory-size

To configure the amount of memory on the security appliance which the various components of WebVPN can access, use the **memory-size** command in webvpn mode. You can configure the amount of memory either as a as a set amount of memory in KB or as a percentage of total memory. To remove a configured memory size, use the **no** form of this command.

Note A reboot is required for the new memory size setting to take effect.

memory-size {percent | kb} *size*

no memory-size [{percent | kb} *size***]**

Syntax Description

kb	Specifies the amount of memory in Kilobytes.
percent	Specifies the amount of memory as a percentage of total memory on the security appliance.
size	Specifies the amount of memory, either in KB or as a percentage of total memory.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The configured amount of memory will be allocated immediately. Before configuring this command, check the amount of available memory by using show memory. If a percentage of total memory is used for configuration, ensure that the configured value is below the available percentage. If a Kilobyte value is used for configuration, ensure that the configured value is below the available amount of memory in Kilobytes.

Examples

The following example shows how to configure a WebVPN memory size of 30 per cent:

```
hostname(config)# webvpn
hostname(config-webvpn)# memory-size percent 30
```

```
hostname(config-webvpn)#
hostname(config-webvpn)# reload
```

Command	Description
show memory webvpn	Displays WebVPN memory usage statistics.

message-length

To filter GTP packets that do not meet the configured maximum and minimum length, use the **message-length** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form to remove the command.

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

Syntax Description

max	Specifies the maximum number of bytes allowed in the UDP payload.
max_bytes	The maximum number of bytes in the UDP payload. The range is from 1 to 65536
min	Specifies the minimum number of bytes allowed in the UDP payload
min_bytes	The minimum number of bytes in the UDP payload. The range is from 1 to 65536

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	No

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The length specified by this command is the sum of the GTP header and the rest of the message, which is the payload of the UDP packet.

Examples

The following example allows messages between 20 bytes and 300 bytes in length:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
hostname(config-gtpmap)#
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

mfib forwarding

To reenable MFIB forwarding on an interface, use the **mfib forwarding** command in interface configuration mode. To disable MFIB forwarding on an interface, use the **no** form of this command.

mfib forwarding

no mfib forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables MFIB forwarding on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

When you enable multicast routing, MFIB forwarding is enabled on all interfaces by default. Use the **no** form of the command to disable MFIB forwarding on a specific interface. Only the **no** form of the command appears in the running configuration.

When MFIB forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when MFIB forwarding is disabled.

Examples

The following example disables MFIB forwarding on the specified interface:

```
hostname(config)# interface GigabitEthernet 0/0
hostname(config-if)# no mfib forwarding
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing.
pim	Enables PIM on an interface.

min-object-size

To set a minimum size for objects that the security appliance can cache for WebVPN sessions, use the min-object-size command in cache mode. To change the size, use the command again. To set no minimum object size, enter a value of zero (0).

min-object-size *integer range*

Syntax Description

integer range	0 - 10000 KB.

Defaults

The default size is 0 KB.

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cache mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The minimum object size must be smaller than the maximum object size. The security appliance calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 40 KB:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# min-object-size 40
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.

Command	Description
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.

mkdir

To create a new directory, use the **mkdir** command in privileged EXEC mode.

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
path	The name and path of the directory to create.

Defaults

If you do not specify a path, the directory is created in the current working directory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If a directory with the same name already exists, then the new directory is not created.

Examples

This example shows how to make a new directory called “backup”:

```
hostname# mkdir backup
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
rmdir	Removes the specified directory.
pwd	Display the current working directory.

mode

To set the security context mode to single or multiple, use the **mode** command in global configuration mode. You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context behaves like an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone appliances. In single mode, the security appliance has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

mode {**single** | **multiple**} [**noconfirm**]

Syntax Description

multiple	Sets multiple context mode.
noconfirm	(Optional) Sets the mode without prompting you for confirmation. This option is useful for automated scripts.
single	Sets the context mode to single.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone device (see the **config-url** command to identify the context configuration location). The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

When you change the context mode using the **mode** command, you are prompted to reboot.

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The security appliance automatically adds an entry for the admin context to the system configuration with the name "admin."

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the security appliance; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device.

Not all features are supported in multiple context mode. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information.

Examples

The following example sets the mode to multiple:

```
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

The following example sets the mode to single:

```
hostname(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....

Booting system, please wait...
```

Related Commands

Command	Description
context	Configures a context in the system configuration and enters context configuration mode.
show mode	Shows the current context mode, either single or multiple.

monitor-interface

To enable health monitoring on a specific interface, use the **monitor-interface** command in global configuration mode. To disable interface monitoring, use the **no** form of this command.

monitor-interface *if_name*

no monitor-interface *if_name*

Syntax Description

if_name	Specifies the name of the interface being monitored.

Defaults

Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged during every interface poll frequency time period between the security appliance failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

In Active/Active failover, this command is only valid within a context.

Examples

The following example enables monitoring on an interface named “inside”:

```
hostname(config)# monitor-interface inside
hostname(config)#
```

Related Commands

Command	Description
clear configure monitor-interface	Restores the default interface health monitoring for all interfaces.
failover interface-policy	Specifies the number or percentage of monitored interface that must fail for failover to occur.
failover polltime	Specifies the interval between hello messages on an interface (Active/Standby failover).
polltime interface	Specifies the interval between hello messages on an interface (Active/Active failover).
show running-config monitor-interface	Displays the **monitor-interface** commands in the running configuration.

more

To display the contents of a file, use the **more** command.

more {/ascii | /binary| /ebcdic | disk0: | disk1: | flash: | **ftp:** | **http:** | **https:** | **system:** | **tftp:}***filename*

Syntax Description

/ascii	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
/ebcdic	(Optional) Displays binary files in EBCDIC.
disk0*:*	(Optional) Displays a file on the internal Flash memory.
disk1:	(Optional) Displays a file on the external Flash memory card.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a web site.
https:	(Optional) Displays a file on a secure web site.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.
filename	Specifies the name of the file to display.

Defaults

ACSII mode

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **more filesystem:** command prompts you to enter the alias of the local directory or file systems.

Examples

This example shows how to display the contents of a local file named “test.cfg”:

```
hostname# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
```

```
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

Command	Description
cd	Changes to the specified directory.
pwd	Displays the current working directory.

mount (CIFS)

To make a Common Internet File System (CIFS) accessible to the security appliance, use the **mount** command in global configuration mode. This command lets you enter config-mount-cifs configuration mode. To un-mount the CIFS network file system, use the **no** form of this command.

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

Syntax Description

domain *domain-name*	(Optional) For CIFS file systems only, this argument specifies the Windows NT domain name. A maximum of 63 characters is permitted.
name	Specifies the name of an existing file system to be assigned to the Local CA.
no	Removes an already mounted CIFS file system and renders it inaccessible.
password *password*	Identifies the authorized password for file-system mounting.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the CIFS file-system server.
share *sharename*	Explicitly identifies a specific server share (a folder) by name to access file data within a server.
status enable/disable	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
type	Specifies the CIFS type of file system to mount. For alternative **type** keywords, refer to the **mount (FTP)** command.
type cifs	Specifies that the file system being mounted is CIFS, a file system that provides volume-mounting capabilities for CIFS-shared directories.
user *username*	The authorized username for file-system mounting.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-mount-cifs configuration	•	•	•	—	•
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **mount** command uses the Installable File System (IFS) to mount the CIFS file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

The **mount** command attaches the CIFS file system on the security appliance to the UNIX file tree. Conversely, the **no mount** command detaches it.

The *mount-name* specified in the **mount** command is used by other CLI commands to refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of an existing mounted file system to save database files to non-flash storage.

The CIFS remote file-access protocol is compatible with the way applications share data on local disks and network file servers. Running over TCP/IP and using the Internet's global DNS, CIFS is an enhanced version of Microsoft's open, cross-platform Server Message Block (SMB) protocol, the native file-sharing protocol in the Windows operating systems.

Always exit from the root shell after using the **mount** command. The **exit** keyword in mount-cifs-config mode returns the user to global configuration mode.

In order to reconnect, remap your connections to storage.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

The following example mounts *cifs://amer;chief:big-boy@myfiler02/my_share* as the label, *cifs_share:*

```
hostname(config)# mount cifs_share type CIFS
hostname (config-mount-cifs)# server myfiler02a
```

Related Commands

Command	Description
debug cifs	Logs CIFS debug messages.
debug ntdomain	Logs Web VPN NT Domain debug messages
debug webvpn cifs	Logs WebVPN CIFS debug messages.
dir all-filesystems	Displays the files of all filesystems mounted on the security appliance.

mount (FTP)

To make a File Transfer Protocol (FTP) file system accessible to the security appliance, use the **mount** *name* **type ftp** command in global configuration mode to enter Mount FTP configuration mode. The **no mount** *name* **type ftp** command is used to un-mount the FTP network file system.

[**no**] **mount** *name* **type FTP server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

Syntax Description

exit	Exit from Mount-FTP Configuration mode and return to Global Configuration mode.
ftp	Specifies that the file system being mounted is FTP, a Linux kernel module, enhancing the Virtual File System (VFS) with FTP volume-mounting capabilities that allow you to mount FTP-shared directories.
mode	Identifies the FTP Transfer Mode as either Active or Passive.
no	Removes an already mounted FTP file system, rendering it inaccessible.
password *password*	Identifies the authorized password for file-system mounting.
path *pathname*	Specifies the directory pathname to the specified FTP file-system server. The pathname cannot contain spaces.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the FTPFS file-system server.
status enable/disable	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
username *username*	Specifies the authorized username for file-system mounting

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-mount-ftp	•	•	•	—	•
Global Configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **mount** *name* **type ftp** command uses the Installable File System (IFS) to mount the specified network file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

To confirm that the FTP file system actually is mounted, use the **dir all-filesystems** instruction

The mount-name specified in the **mount** command is used when other CLI commands refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of a mounted file system to save database files to non-flash storage.

Note Using the **mount** command when you create an FTP-type mount requires that the FTP Server must have a UNIX directory listing style. Microsoft FTP servers have a default of MS-DOS directory listing style.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

This example mounts *ftp://amor;chief:big-kid@myfiler02* as the label, *my ftp:*

```
hostname(config)# mount myftp type ftp server myfiler02a path status enable username
chief password big-kid
```

Related Commands

Command	Description
debug webvpn	Logs WebVPN debug messages.
ftp mode passive	Controls interaction between the FTP client on the security appliance and the FTP server.

mroute

To configure a static multicast route, use the **mroute** command in global configuration mode. To remove a static multicast route, use the **no** form of this command.

mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

Syntax Description

dense *output_if_name*	(Optional) The interface name for dense mode output. The **dense** *output_if_name* keyword and argument pair is only supported for SMR stub multicast routing (igmp forwarding).
distance	(Optional) The administrative distance of the route. Routes with lower distances have preference. The default is 0.
in_if_name	Specifies the incoming interface name for the mroute.
rpf_addr	Specifies the incoming interface for the mroute. If the RPF address PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-addr* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system.
smask	Specifies the multicast source network address mask.
src	Specifies the IP address of the multicast source.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command lets you statically configure where multicast sources are located. The security appliance expects to receive multicast packets on the same interface as it would use to send unicast packets to a specific source. In some cases, such as bypassing a route that does not support multicast routing, multicast packets may take a different path than the unicast packets.

Static multicast routes are not advertised or redistributed.

Use the **show mroute** command displays the contents of the multicast route table. Use the **show running-config mroute** command to display the mroute commands in the running configuration.

Examples

The following example shows how configure a static multicast route using the **mroute** command:

```
hostname(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the configuration.
show mroute	Displays the IPv4 multicast routing table.
show running-config mroute	Displays the **mroute** commands in the configuration.

msie-proxy except-list

To configure Microsoft Internet Explorer browser proxy exception list settings for a local bypass on the client PC, enter the **msie-proxy except-list** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

Syntax Description

none	Indicates that there is no IP address/hostname or port and prevents inheriting an exception list.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client PC. The port num ber is optional.

Defaults

By default, msie-proxy except-list is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Examples

The following example shows how to set a Microsoft Internet Explorer proxy exception list, consisting of the server at IP address 192.168.20.1, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy local-bypass

To configure Microsoft Internet Explorer browser proxy local-bypass settings for a client PC, enter the **msie-proxy local-bypass** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

Syntax Description

disable	Disables Microsoft Internet Explorer browser proxy local-bypass settings for a client PC.
enable	Enables Microsoft Internet Explorer browser proxy local-bypass settings for a client PC.

Defaults

By default, msie-proxy local-bypass is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable Microsoft Internet Explorer proxy local-bypass for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy method

To configure the browser proxy actions (“methods”) for a client PC, enter the **msie-proxy method** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

Note See the Usage Guidelines section for qualifications that apply to this syntax.

Syntax Description

auto-detect	Enables the use of automatic proxy server detection in Internet Explorer or Firefox for the client PC.
no-modify	Leaves the HTTP browser proxy server setting in the browser unchanged for this client PC.
no-proxy	Disables the HTTP proxy setting in the browser for the client PC.
use-pac-url	Directs Internet Explorer to retrieve the HTTP proxy server setting from the proxy auto-configuration file URL specified in the **msie-proxy pac-url** command. This option is valid only for Internet Explorer.
use-server	Sets the HTTP proxy server setting in the browser to use the value configured in the **msie-proxy server** command.

Defaults

The default method is use-server.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Added the use-pac-url option.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number can contain up to 100 characters.

The Safari browser does not support auto-detect. The Firefox and Safari browsers support the use of only one of these command options at a time. Microsoft Internet Explorer supports the following combinations of options for this command:

[no] msie-proxy method no-proxy

[no] msie-proxy method no-modify

[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. The .pac file resides on a web server. When you specify **use-pac-url**, Internet Explorer uses the .pac file to determine the proxy settings. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file. For details about .pac files, see the following Microsoft Knowledge Base article: http://www.microsoft.com/mind/0599/faq/faq0599.asp.

Examples

The following example shows how to configure auto-detect as the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

The following example configures the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup to use the server QAserver, port 1001 as the server for the client PC:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file.
msie-proxy server	Configures a Microsoft Internet Explorer browser proxy server and port for a client PC.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy pac-url

To tell a browser where to look for proxy information, enter the **msie-proxy pac-url** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

Syntax Description

none	Specifies that there is no URL value.
value *url*	Specifies the URL of the website at which the browser can get the proxy auto-configuration file that defines the proxy server or servers to use.

Defaults

The default value is none.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Requirements

To use the proxy auto-configuration feature, the remote user must use the Cisco AnyConnect VPN Client. To enable the use of the proxy auto-configuration URL, you must also configure the **msie-proxy method** command with the **use-pac-url** option.

Why Use This Command

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.
- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

How to Use the Proxy Auto-Configuration Feature

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file. Then, when you specify **use-pac-url** in the **msie-proxy method** command, the browser uses the .pac file to determine the proxy settings. For details about .pac files, see the following Microsoft Knowledge Base article: http://www.microsoft.com/mind/0599/faq/faq0599.asp.

Examples

The following example shows how to configure a browser to get its proxy setting from the URL www.mycompanyserver.com for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url value http://www.mycompanyserver.com
hostname(config-group-policy)#
```

The following example disables the proxy auto-configuration feature for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url none
hostname(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy method	Configures the browser proxy actions (“methods”) for a client PC.
msie-proxy server	Configures a Microsoft Internet Explorer browser proxy server and port for a client PC.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy server

To configure a Microsoft Internet Explorer browser proxy server and port for a client PC, enter the **msie-proxy server** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

Syntax Description

none	Indicates that there is no IP address/hostname or port specified for the proxy server and prevents inheriting a server.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client PC. The port number is optional.

Defaults

By default, no msie-proxy server is specified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Examples

The following example shows how to configure the IP address 192.168.10.1 as a Microsoft Internet Explorer proxy server, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

mtu

To specify the maximum transmission unit for an interface, use the **mtu** command in global configuration mode. To reset the MTU block size to 1500 for Ethernet interfaces, use the **no** form of this command. This command supports IPv4 and IPv6 traffic.

mtu *interface_name bytes*

no mtu *interface_name bytes*

Syntax Description

bytes	Number of bytes in the MTU; valid values are from 64 to 65,535 bytes.
interface_name	Internal or external network interface name.

Defaults

The default *bytes* is 1500 for Ethernet interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	—	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **mtu** command lets you to set the data size that is sent on a connection. Data that is larger than the MTU value is fragmented before being sent.

The security appliance supports IP path MTU discovery (as defined in RFC 1191), which allows a host to dynamically discover and cope with the differences in the maximum allowable MTU size of the various links along the path. Sometimes, the security appliance cannot forward a datagram because the packet is larger than the MTU that you set for the interface, but the “don’t fragment” (DF) bit is set. The network software sends a message to the sending host, alerting it to the problem. The host has to fragment packets for the destination so that they fit the smallest packet size of all the links along the path.

The default MTU is 1500 bytes in a block for Ethernet interfaces (which is also the maximum). This value is sufficient for most applications, but you can pick a lower number if network conditions require it.

When using the Layer 2 Tunneling Protocol (L2TP), we recommend that you set the MTU size to 1380 to account for the L2TP header and IPSec header length.

Examples

This example shows how to specify the MTU for an interface:

```
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
hostname(config)# mtu inside 8192
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
show running-config mtu	Displays the current maximum transmission unit block size.

multicast boundary

To configure a multicast boundary for administratively-scoped multicast addresses, use the **multicast boundary** command in interface configuration mode. To remove the boundary, use the **no** form of this command. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains.

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

Syntax Description

acl	Specifies an access list name or number. The access list defines the range of addresses affected by the boundary. Use only standard ACLs with this command; extended ACLs are not supported.
filter-autorp	Filters Auto-RP messages denied by the boundary ACL. If not specified, all Auto-RP messages are passed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command to configure an administratively scoped boundary on an interface to filter multicast group addresses in the range defined by the *acl* argument. A standard access list defines the range of addresses affected. When this command is configured, no multicast data packets are allowed to flow across the boundary in either direction. Restricting multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Examples

The following example sets up a boundary for all administratively scoped addresses and filters the Auto-RP messages:

```
hostname(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
hostname(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

multicast-routing

To enable IP multicast routing on the security appliance, use the **multicast routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

multicast-routing

no multicast-routing

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM and IGMP on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **multicast-routing** command enables PIM and IGMP on all interfaces.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

If the security appliance is the PIM RP, use the untranslated outside address of the security appliance as the RP address.

The number of entries in the multicast routing tables are limited by the amount of RAM on the system. Table 20-3 lists the maximum number of entries for specific multicast tables based on the amount of RAM on the security appliance. Once these limits are reached, any new entries are discarded.

Table 20-3 Entry Limits for Multicast Tables

Table	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP Groups	1000	3000	5000
PIM Routes	3000	7000	12000

Examples

The following example enables IP multicast routing on the security appliance:

```
hostname(config)# multicast-routing
```

Related Commands

Command	Description
igmp	Enables IGMP on an interface.
pim	Enables PIM on an interface.

CHAPTER 21

nac policy through override-svc-download Commands

nac-policy

To create or access a Cisco Network Admission Control (NAC) policy, and specify its type, use the **nac-policy** command in global configuration mode. To remove the NAC policy from the configuration, use the **no** form of this command.

nac-policy *nac-policy-name* **nac-framework**

[**no**] **nac-policy** *nac-policy-name* **nac-framework**

Syntax Description

nac-policy-name	Name of the NAC policy. Enter a string of up to 64 characters to name the NAC policy. The **show running-config nac-policy** command displays the name and configuration of each NAC policy already present on the security appliance.
nac-framework	Specifies the use of a NAC framework to provide a network access policy for remote hosts. A Cisco Access Control Server must be present on the network to provide NAC Framework services for the security appliance. If you specify this type, the prompt indicates you are in config--nac-policy-nac-framework configuration mode. This mode lets you configure the NAC Framework policy.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use this command once for each NAC Appliance to be assigned to a group policy. Then use the **nac-settings** command to assign the NAC policy to each applicable group policy. Upon the setup of an IPSec or Cisco AnyConnect VPN tunnel, the security appliance applies the NAC policy associated with the group policy in use.

You cannot use the **no nac-policy** *name* command to remove a NAC policy if it is already assigned to one or more group policies.

Examples

The following command creates and accesses a NAC Framework policy named nac-framework1:

```
hostname(config)# nac-policy nac-framework1 nac-framework
hostname(config-nac-policy-nac-framework)
```

The following command removes the NAC Framework policy named nac-framework1:

```
hostname(config)# no nac-policy nac-framework1
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
show running-config nac-policy	Displays the configuration of each NAC policy on the security appliance.
show nac-policy	Displays NAC policy usage statistics on the security appliance.
clear nac-policy	Resets the NAC policy usage statistics.
nac-settings	Assigns a NAC policy to a group policy.
clear configure nac-policy	Removes all NAC policies from the running configuration except for those that are assigned to group policies.

nac-settings

To assign a NAC policy to a group policy, use the **nac-settings** command in group-policy configuration mode, as follows:

nac-settings {**value** *nac-policy-name* | **none**}

[**no**] **nac-settings** {**value** *nac-policy-name* | **none**}

Syntax Description

nac-policy-name	NAC policy to be assigned to the group policy. The NAC policy you name must be present in the configuration of the security appliance. The **show running-config nac-policy** command displays the name and configuration of each NAC policy.
none	Removes the *nac-policy-name* from the group policy and disables the use of a NAC policy for this group policy. The group policy does not inherit the nac-settings value from the default group policy.
value	Assigns the NAC policy to be named to the group policy.

Defaults

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **nac-policy** command to specify the name and type of the NAC policy, then use this command to assign it to a group policy.

The **show running-config nac-policy** command displays the name and configuration of each NAC policy.

The security appliance automatically enables NAC for a group policy when you assign a NAC policy to it.

Examples

The following command removes the *nac-policy-name* from the group policy. The group policy inherits the *nac-settings* value from the default group policy:

```
hostname(config-group-policy)# no nac-settings
```

```
hostname(config-group-policy)
```

The following command removes the *nac-policy-name* from the group policy and disables the use of a NAC policy for this group policy. The group policy does not inherit the nac-settings value from the default group policy.

```
hostname(config-group-policy)# nac-settings none
hostname(config-group-policy)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
show running-config nac-policy	Displays the configuration of each NAC policy on the security appliance.
show nac-policy	Displays NAC policy usage statistics on the security appliance.
show vpn-session_summary.db	Displays the number IPSec, WebVPN, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

name

To associate a name with an IP address, use the **name** command in global configuration mode. To disable the use of the text names but not remove them from the configuration, use the **no** form of this command.

name *ip_address name* [description *text*]]

no name *ip_address* **[***name* [description *text***]]**

Syntax Description

description	(Optional) Specifies a description for the ip address name.
ip_address	Specifies an IP address of the host that is named.
name	Specifies the name assigned to the IP address. Use characters a to z, A to Z, 0 to 9, a dash, and an underscore. The *name* must be 63 characters or less. Also, the *name* cannot start with a number.
text	Specifies the text for the description.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexissting.
7.0(4)	This command was enhanced to include an optional description.

Usage Guidelines

To enable the association of a name with an IP address, use the **names** command. You can associate only one name with an IP address.

You must first use the **names** command before you use the **name** command. Use the **name** command immediately after you use the **names** command and before you use the **write memory** command.

The **name** command lets you identify a host by a text name and map text strings to IP addresses. The **no name** command allows you to disable the use of the text names but does not remove them from the configuration. Use the **clear configure name** command to clear the list of names from the configuration.

To disable displaying **name** values, use the **no names** command.

Both the **name** and **names** commands are saved in the configuration.

The **name** command does not support assigning a name to a network mask. For example, this command would be rejected:

```
hostname(config)# name 255.255.255.0 class-C-mask
```

Note None of the commands in which a mask is required can process a name as an accepted network mask.

Examples

This example shows that the **names** command allows you to enable use of the **name** command. The **name** command substitutes **sa_inside** for references to 192.168.42.3 and **sa_outside** for 209.165.201.3. You can use these names with the **ip address** commands when assigning IP addresses to the network interfaces. The **no names** command disables the **name** command values from displaying. Subsequent use of the **names** command again restores the **name** command value display.

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

hostname(config)# no names
hostname(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

hostname(config)# names
hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
names	Enables the association of a name with an IP address.
show running-config name	Displays the names associated with an IP address.

nameif

To provide a name for an interface, use the **nameif** command in interface configuration mode. To remove the name, use the **no** form of this command. The interface name is used in all configuration commands on the security appliance instead of the interface type and ID (such as gigabitethernet0/1), and is therefore required before traffic can pass through the interface.

nameif *name*

no nameif

Syntax Description

name	Sets a name up to 48 characters in length. The name is not case-sensitive.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

For subinterfaces, you must assign a VLAN with the **vlan** command before you enter the **nameif** command.

You can change the name by reentering this command with a new value. Do not enter the **no** form, because that command causes all commands that refer to that name to be deleted.

Examples

The following example configures the names for two interfaces to be “inside” and “outside:”

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/0
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.
security-level	Sets the security level for the interface.
vlan	Assigns a VLAN ID to a subinterface.

names

To enable the association of a name with an IP address, use the **names** command in global configuration mode. You can associate only one name with an IP address. To disable displaying **name** values, use the **no names** command.

names

no names

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **names** command is used to enable the association of a name with an IP address that you configured with the **name** command. The order in which you enter the **name** or **names** commands is irrelevant.

Examples

The following example shows how to enable the association of a name with an IP address:

```
hostname(config)# names
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.
show running-config name	Displays a list of names associated with IP addresses.
show running-config names	Displays the IP address-to-name conversions.

name-separator

To specify a character as a delimiter between the e-mail and VPN username and password, use the **name-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the **no** version of this command.

name-separator [*symbol*]

no name-separator

Syntax Description

symbol	(Optional) The character that separates the e-mail and VPN usernames and passwords. Choices are "@," (at) "|" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Defaults

The default is ":" (colon).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The name separator must be different from the server separator.

Examples

The following example shows how to set a hash (#) as the name separator for POP3S:

```
hostname(config)# pop3s
hostname(config-pop3s)# name-separator #
```

Related Commands

Command	Description
server-separator	Separates the e-mail and server names.

name-server

To identify one or more DNS servers, use the **name-server** command in dns server-group configuration mode. To remove a server or servers, use the **no** form of this command. The security appliance uses DNS to resolve server names in your SSL VPN configuration or certificate configuration (see "Usage Guidelines" for a list of supported commands). Other features that define server names (such as AAA) do not support DNS resolution. You must enter the IP address or manually resolve the name to an IP address by using the **name** command.

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

Syntax Description

ip_address	Specifies the DNS server IP address. You can specify up to six addresses as separate commands, or for convenience, up to six addresses in one command separated by spaces. If you enter multiple servers in one command, the security appliance saves each server in a separate command in the configuration. The security appliance tries each DNS server in order until it receives a response.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
dns server-group configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

To enable DNS lookup, configure the **domain-name** command in dns server-group configuration mode. If you do not enable DNS lookup, the DNS servers are not used.

SSL VPN commands that support DNS resolution include the following:

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**
- **url-list**

Certificate commands that support DNS resolution include the following:

- **enrollment url**
- **url**

You can manually enter names and IP addresses using the **name** command.

Examples

The following example adds three DNS servers to the group "dnsgroup1":

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

The security appliance saves the configuration as separate commands, as follows:

```
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
```

To add two additional servers, you can enter them as one command:

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

To verify the dns server group configuration, enter the **show running-config dns** command in global configuration mode:

```
hostname(config)# show running-config dns
name-server 10.1.1.1
name-server 10.2.3.4
name-server 192.168.5.5
name-server 10.5.1.1
name-server 10.8.3.8
...
```

Or you can enter them as two separate commands:

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# name-server 10.5.1.1
hostname(config)# name-server 10.8.3.8
```

To delete multiple servers you can enter them as multiple commands or as one command, as follows:

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# no name-server 10.5.1.1 10.8.3.8
```

Related Commands

Command	Description
domain-name	Sets the default domain name.
retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
timeout	Specifies the amount of time to wait before trying the next DNS server.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

nat

To identify addresses on one interface that are translated to mapped addresses on another interface, use the **nat** command in global configuration mode. This command configures dynamic NAT or PAT, where an address is translated to one of a pool of mapped addresses. To remove the **nat** command, use the **no** form of this command.

For regular dynamic NAT:

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

For policy dynamic NAT and NAT exemption:

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

Syntax Description

access-list *access_list_name*	Identifies the local addresses and destination addresses using an extended access list, also known as policy NAT. Create the access list using the **access-list** command. You can optionally specify the local and destination ports in the access list using the **eq** operator. If the NAT ID is **0**, then the access list specifies addresses that are exempt from NAT. NAT exemption is not the same as policy NAT; you cannot specify the port addresses, for example. **Note** Access list hit counts, as shown by the **show access-list** command, do not increment for NAT exemption access lists.
dns	(Optional) Rewrites the A record, or address record, in DNS replies that match this command. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value. If your NAT statement includes the address of a host that has an entry in a DNS server, and the DNS server is on a different interface from a client, then the client and the DNS server need different addresses for the host; one needs the global address and one needs the local address.The translated host needs to be on the same interface as either the client or the DNS server. Typically, hosts that need to allow access from other interfaces use a static translation, so this option is more likely to be used with the **static** command.

emb_limit	(Optional) Specifies the maximum number of embryonic connections per host. The default is 0, which means unlimited embryonic connections. Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. Not supported for NAT exemption (**nat 0 access-list**). Although you can enter this argument at the CLI, it is not saved to the configuration.
mask	(Optional) Specifies the subnet mask for the real addresses. If you do not enter a mask, then the default mask for the IP address class is used.
nat_id	Specifies an integer for the NAT ID. For regular NAT, this integer is between 1 and 2147483647. For policy NAT (nat id access-list), this integer is between 1 and 65535. Identity NAT (**nat 0**) and NAT exemption (**nat 0 access-list**) use the NAT ID of **0**. This ID is referenced by the **global** command to associate a global pool with the *real_ip*.
norandomseq	(Optional) Disables TCP ISN randomization protection. Not supported for NAT exemption (**nat 0 access-list**). Although you can enter this argument at the CLI, it is not saved to the configuration. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions. Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session. TCP initial sequence number randomization can be disabled if required. For example: • If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic. • If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
outside	(Optional) If this interface is on a lower security level than the interface you identify by the matching **global** statement, then you must enter **outside**. This feature is called outside NAT or bidirectional NAT.
real_ifc	Specifies the name of the interface connected to the real IP address network.
real_ip	Specifies the real address that you want to translate. You can use **0.0.0.0** (or the abbreviation **0**) to specify all addresses.

tcp *tcp_max_conns*	(Optional) Specifies the maximum number of simultaneous TCP connections allowed to the local-host (see the **local-host** command). The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the module policy framework by setting a connection-limit on a class within a policy-map. Not supported for NAT exemption (**nat 0 access-list**). Although you can enter this argument at the CLI, it is not saved to the configuration.
udp *udp_max_conns*	(Optional) Specifies the maximum number of simultaneous UDP connections allowed to the local-host (see the **local-host** command). The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the module policy framework by setting a connection-limit on a class within a policy-map. Not supported for NAT exemption (**nat 0 access-list**). Although you can enter this argument at the CLI, it is not saved to the configuration.

Defaults

The default value for *tcp_max_conns*, *emb_limit*, and *udp_max_conns* is 0 (unlimited), which is the maximum available.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	NAT is now supported in transparent firewall mode.

Usage Guidelines

For dynamic NAT and PAT, you first configure a **nat** command identifying the real addresses on a given interface that you want to translate. Then you configure a separate **global** command to specify the mapped addresses when exiting another interface (in the case of PAT, this is one address). Each **nat** command matches a **global** command by comparing the NAT ID, a number that you assign to each command.

NAT Control

The security appliance translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet continues. The exception is when you enable NAT control using the **nat-control** command. NAT control requires that packets traversing from a higher security interface

(inside) to a lower security interface (outside) match a NAT rule, or else processing for the packet stops. NAT is not required between same security level interfaces even if you enable NAT control. You can optionally configure NAT if desired.

Dynamic NAT Overview

Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool can include fewer addresses than the real group. When a host you want to translate accesses the destination network, the security appliance assigns it an IP address from the mapped pool. The translation is added only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out (see the **timeout xlate** command). Users on the destination network, therefore, cannot reliably initiate a connection to a host that uses dynamic NAT (or PAT, even if the connection is allowed by an access list), and the security appliance rejects any attempt to connect to a real host address directly. See the **static** command for reliable access to hosts.

Dynamic NAT Advantages and Disadvantages

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

  Use PAT if this event occurs often, because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool; if the destination network requires registered addresses, such as the Internet, you might encounter a shortage of usable addresses.

The advantage of dynamic NAT is that some protocols cannot use PAT. For example, PAT does not work with IP protocols that do not have a port to overload, such as GRE version 0. PAT also does not work with some applications that have a data stream on one port and the control path on another and are not open standard, such as some multimedia applications.

Dynamic PAT Overview

PAT translates multiple real addresses to a single mapped IP address. Specifically, the security appliance translates the real address and source port (real socket) to the mapped address and a unique port above 1024 (mapped socket). Each connection requires a separate translation, because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

After the connection expires, the port translation also expires after 30 seconds of inactivity. The timeout is not configurable.

PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the security appliance interface IP address as the PAT address. PAT does not work with some multimedia applications that have a data stream that is different from the control path.

Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access list allows it. Because the address (both real and mapped) is unpredictable, a connection to the host is unlikely. However in this case, you can rely on the security of the access list.

Bypassing NAT

If you enable NAT control, then inside hosts must match a NAT rule when accessing outside hosts. If you do not want to perform NAT for some hosts, then you can bypass NAT for those hosts (alternatively, you can disable NAT control). You might want to bypass NAT, for example, if you are using an application that does not support NAT. You can use the **static** command to bypass NAT, or one of the following options:

- Identity NAT (**nat 0** command)—When you configure identity NAT (which is similar to dynamic NAT), you do not limit translation for a host on specific interfaces; you must use identity NAT for connections through all interfaces. Therefore, you cannot choose to perform normal translation on real addresses when you access interface A, but use identity NAT when accessing interface B. Regular dynamic NAT, on the other hand, lets you specify a particular interface on which to translate the addresses. Make sure that the real addresses for which you use identity NAT are routable on all networks that are available according to your access lists.

  For identity NAT, even though the mapped address is the same as the real address, you cannot initiate a connection from the outside to the inside (even if the interface access list allows it). Use static identity NAT or NAT exemption for this functionality.

- NAT exemption (**nat 0 access-list** command)—NAT exemption allows both translated and remote hosts to initiate connections. Like identity NAT, you do not limit translation for a host on specific interfaces; you must use NAT exemption for connections through all interfaces. However, NAT exemption does let you specify the real and destination addresses when determining the real addresses to translate (similar to policy NAT), so you have greater control using NAT exemption. However unlike policy NAT, NAT exemption does not consider the ports in the access list. NAT exemption also does not support connection settings such as the **tcp** and **udp** keywords.

Policy NAT

Policy NAT lets you identify real addresses for address translation by specifying the source and destination addresses in an extended access list. You can also optionally specify the source and destination ports. Regular NAT can only consider the real addresses. For example, you can translate the real address to mapped address A when it accesses server A, but translate the real address to mapped address B when it accesses server B.

When you specify the ports in policy NAT for applications that require application inspection for secondary channels (FTP, VoIP, etc.), the security appliance automatically translates the secondary ports.

Note All types of NAT support policy NAT except for NAT exemption. NAT exemption uses an access list to identify the real addresses, but differs from policy NAT in that the ports are not considered. You can accomplish the same result as NAT exemption using **static** identity NAT, which does support policy NAT.

Connection Settings Using the Modular Policy Framework

You can alternatively set connection limits (but not embryonic connection limits) using the Modular Policy Framework. See the **set connection** commands for more information. You can only set embryonic connection limits using NAT. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

Clearing Translation Sessions

If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using **clear xlate** command. However, clearing the translation table disconnects all of the current connections.

Examples

For example, to translate the 10.1.1.0/24 network on the inside interface, enter the following command:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

To identify a pool of addresses for dynamic NAT as well as a PAT address for when the NAT pool is exhausted, enter the following commands:

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

To translate the lower security dmz network addresses so they appear to be on the same network as the inside network (10.1.1.0), for example, to simplify routing, enter the following commands:

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

To identify a single real address with two different destination addresses using policy NAT, enter the following commands:

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

To identify a single real address/destination address pair that use different ports using policy NAT, enter the following commands:

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

Related Commands

Command	Description
access-list deny-flow-max	Specifies the maximum number of concurrent deny flows that can be created.
clear configure nat	Removes the NAT configuration.
global	Creates entries from a pool of global addresses.
interface	Creates and configures an interface.
show running-config nat	Displays a pool of global IP addresses that are associated with the network.

nat (vpn load-balancing)

To set the IP address to which NAT translates the IP address of this device, use the **nat** command in VPN load-balancing configuration mode. To disable this NAT translation, use the **no** form of this command.

nat *ip-address*

no nat [*ip-adddress*]

Syntax Description

ip-address	The IP address to which you want this NAT to translate the IP address of this device.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
VPN load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

In the **no nat** form of the command, if you specify the optional *ip-address* value, the IP address must match the existing NAT IP address in the running configuration.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **nat** command that sets the NAT-translated address to 192.168.10.10:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
```

```
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

Related Commandsh

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

nat-control

To enforce NAT control use the **nat-control** command in global configuration mode. NAT control requires NAT for inside hosts when they access the outside. To disable NAT control, use the **no** form of this command.

nat-control

no nat-control

Syntax Description

This command has no arguments or keywords.

Defaults

NAT control is disabled by default (**no nat-control** command). If you upgraded from an earlier version of software, however, NAT control might be enabled on your system because it was the default in some earlier versions.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.3.(1)	NAT is now supported in transparent firewall mode.

Usage Guidelines

NAT control requires that packets traversing from an inside interface to an outside interface match a NAT rule; for any host on the inside network to access a host on the outside network, you must configure NAT to translate the inside host address.

Interfaces at the same security level are not required to use NAT to communicate. However, if you configure dynamic NAT or PAT on a same security interface with NAT control enabled, then all traffic from the interface to a same security interface or an outside interface must match a NAT rule.

Similarly, if you enable outside dynamic NAT or PAT with NAT control, then all outside traffic must match a NAT rule when it accesses an inside interface.

Static NAT with NAT control does not cause these restrictions.

By default, NAT control is disabled, so you do not need to perform NAT on any networks unless you choose to perform NAT.

Note In multiple context mode, the packet classifier relies on the NAT configuration in some cases to assign packets to contexts. If you do not perform NAT because NAT control is disabled, then the classifier might require changes in your network configuration.

If you want the added security of NAT control but do not want to translate inside addresses in some cases, you can apply a NAT exemption (**nat 0 access-list**) or identity NAT (**nat 0** or **static**) rule on those addresses.

When NAT control is disabled with the **no nat control** command, and a NAT and a global command pair are configured for an interface, the real IP addresses cannot go out on other interfaces unless you define those destinations with the **nat 0 access-list** command.

For example, the following NAT is the that one you want performed when going to the outside network:

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
```

The above configuration catches everything on the inside network, so if you do not want to translate inside addresses when they go to the DMZ, then you need to match that traffic for NAT exemption, as shown in the following example:

```
access-list EXEMPT extended permit ip any 192.168.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
access-list EXEMPT extended permit ip any 10.1.1.0 255.255.255.0
access-list EXEMPT remark This matches any traffic going to DMZ1
nat (inside) 0 access-list EXEMPT
```

Alternately, you can perform NAT translation on all interfaces:

```
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 209.165.201.2
global (dmz1) 1 192.168.1.230
global (dmz2) 1 10.1.1.230
```

Examples

The following example enables NAT control:

```
hostname(config)# nat-control
```

Related Commands

Command	Description
nat	Defines an address on one interface that is translated to a mapped address on another interface.
show running-config nat-control	Shows the NAT configuration requirement.
static	Translates a real address to a mapped address.

nat-rewrite

To enable NAT rewrite for IP addressess embedded in the A-record of a DNS response, use the **nat-rewrite** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

nat-rewrite

no nat-rewrite

Syntax Description

This command has no arguments or keywords.

Defaults

NAT rewrite is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no nat-rewrite** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This feature performs NAT translation of A-type Resource Record (RR) in a DNS response.

Examples

The following example shows how to enable NAT rewrite in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# nat-rewrite
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

nbns-server (tunnel-group webvpn attributes mode)

To configure an NBNS server, use the **nbns-server** command in tunnel-group webvpn configuration mode. To remove the NBNS server from the configuration, use the **no** form of this command.

The security appliance queries NBNS servers to map NetBIOS names to IP addresses. WebVPN requires NetBIOS to access or share files on remote systems.

nbns-server {*ipaddr* | *hostname***}** [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

Syntax Description

hostname	Specifies the hostname for the NBNS server.
ipaddr	Specifies the IP address for the NBNS server.
master	Indicates that this is a master browser, rather than a WINS server.
retry	Indicates that a retry value follows.
retries	Specifies the number of times to retry queries to NBNS servers. The security appliance recycles through the list of servers the number of times you specify here before sending an error message. The default value is 2; the range is 1 through 10.
timeout	Indicates that a timeout value follows.
timeout	Specifies the amount of time the security appliance waits before sending the query again, to the same server if there is only one, or another server if there are multiple NBNS servers. The default timeout is 2 seconds; the range is 1 to 30 seconds.

Defaults

No NBNS server is configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Moved from webvpn mode to tunnel-group webvpn configuration mode.

Usage Guidelines

In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group webvpn-attributes configuration mode.

Maximum of 3 server entries. The first server you configure is the primary server, and the others are backups, for redundancy.

Use the **no** option to remove the matching entry from the configuration.

Examples

The following example shows how to configure the tunnel-group "test" with an NBNS server that is a master browser with an IP address of 10.10.10.19, a timeout value of 10 seconds, and 8 retries. It also shows how to configure an NBNS WINS server with an IP address of 10.10.10.24, a timeout value of 15 seconds, and 8 retries.

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
tunnel-group webvpn-attributes	Specifies the WebVPN attributes for the named tunnel-group.

nbns-server (webvpn mode)

To configure an NBNS server, use the **nbns-server** command in tunnel-group webvpn configuration mode. To remove the NBNS server from the configuration, use the **no** form of this command.

The security appliance queries NBNS servers to map NetBIOS names to IP addresses. WebVPN requires NetBIOS to access or share files on remote systems.

nbns-server {*ipaddr* | *hostname***}** [**master**] [**timeout** *timeout*] [**retry** *retries*]

no nbns-server

Syntax Description

hostname	Specifies the hostname for the NBNS server.
ipaddr	Specifies the IP address for the NBNS server.
master	Indicates that this is a master browser, rather than a WINS server.
retry	Indicates that a retry value follows.
retries	Specifies the number of times to retry queries to NBNS servers. The security appliance recycles through the list of servers the number of times you specify here before sending an error message. The default value is 2; the range is 1 through 10.
timeout	Indicates that a timeout value follows.
timeout	Specifies the amount of time the security appliance waits before sending the query again, to the same server if there is only one, or another server if there are multiple NBNS servers. The default timeout is 2 seconds; the range is 1 to 30 seconds.

Defaults

No NBNS server is configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Moved from webvpn mode to tunnel-group webvpn configuration mode.

Usage Guidelines

This command is deprecated in webvpn configuration mode. The nbns-server command in tunnel-group webvpn-attributes configuration mode replaces it. In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group webvpn-attributes mode.

Maximum of 3 server entries. The first server you configure is the primary server, and the others are backups, for redundancy.

Use the **no** option to remove the matching entry from the configuration.

Examples

The following example shows how to configure an NBNS server that is a master browser with an IP address of 10.10.10.19, a timeout value of 10 seconds, and 8 retries. It also shows how to configure an NBNS WINS server with an IP address of 10.10.10.24, a timeout value of 15 seconds, and 8 retries.

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

To define a static neighbor on a point-to-point, non-broadcast network, use the **neighbor** command in router configuration mode. To remove the statically defined neighbor from the configuration, use the **no** form of this command. The **neighbor** command is used to advertise OSPF routes over VPN tunnels.

neighbor *ip_address* [**interface** *name*]

no neighbor *ip_address* [**interface** *name*]

Syntax Description

interface *name*	(Optional) The interface name, as specified by the **nameif** command, through which the neighbor can be reached.
ip_address	IP address of the neighbor router.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

One neighbor entry must be included for each known non-broadcast network neighbor. The neighbor address must be on the primary address of the interface.

The **interface** option needs to be specified when the neighbor is not on the same network as any of the directly connected interfaces of the system. Additionally, a static route must be created to reach the neighbor.

Examples

The following example defines a neighbor router with an address of 192.168.1.1:

```
hostname(config-router)# neighbor 192.168.1.1
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

neighbor (EIGRP)

To define an EIGRP neighbor router with which to exchange routing information, use the **neighbor** command in router configuration mode. To remove a neighbor entry, use the **no** form of this command.

neighbor *ip_address* **interface** *name*

no neighbor *ip_address* **interface** *name*

Syntax Description

interface *name*	The interface name, as specified by the **nameif** command, through which the neighbor can be reached.
ip_address	IP address of the neighbor router.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use multiple neighbor statements to establish peering sessions with specific EIGRP neighbors. The interface through which EIGRP exchanges routing updates must be specified in the neighbor statement. The interfaces through which two EIGRP neighbors exchange routing updates must be configured with IP addresses from the same network.

Note Configuring the **passive-interface** command for an interface suppresses all incoming and outgoing routing updates and hello messages on that interface. EIGRP neighbor adjacencies cannot be established or maintained over an interface that is configured as passive.

EIGRP hello messages are sent as unicast messages to neighbors defined using the **neighbor** command.

Examples

The following example configures EIGRP peering sessions with the 192.168.1.1 and 192.168.2.2 neighbors:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.0.0
```

```
hostname(config-router)# neighbor 192.168.1.1 interface outside
hostname(config-router)# neighbor 192.168.2.2 interface branch_office
```

Related Commands

Command	Description
debug eigrp neighbors	Displays debug information for EIGRP neighbor messages.
show eigrp neighbors	Displays the EIGRP neighbor table.

nem

To enable network extension mode for hardware clients, use the **nem enable** command in group-policy configuration mode. To disable NEM, use the **nem disable** command. To remove the NEM attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy.

nem {**enable | disable**}

no nem

Syntax Description

disable	Disables Network Extension Mode.
enable	Enables Network Extension Mode.

Defaults

Network extension mode is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policyconfiguration	•	—	•	—	—

Usage Guidelines

Network Extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance. PAT does not apply. Therefore, devices behind the security appliance have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel, but after the tunnel is up, either side can initiate data exchange.

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set NEM for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

network

To specify a list of networks for the RIP routing process, use the **network** command in router configuration mode. To remove a network definition, use the **no** form of this command.

network *ip_addr*

no network *ip_addr*

Syntax Description

ip_addr	The IP address of a directly connected network. The interface connected to the specified network will participate in the RIP routing process.

Defaults

No networks are specified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The network number specified must not contain any subnet information. There is no limit to the number of network commands you can use on the router. RIP routing updates will be sent and received only through interfaces on the specified networks. Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

Examples

The following example defines RIP as the routing protocol to be used on all interfaces connected to networks 10.0.0.0 and 192.168.7.0:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# network 192.168.7.0
```

Related Commands

Command	Description
router rip	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

network (EIGRP)

To specify a list of networks for the EIGRP routing process, use the **network** command in router configuration mode. To remove a network definition, use the **no** form of this command.

network *ip_addr* [*mask*]

no network *ip_addr* [*mask*]

Syntax Description

ip_addr	The IP address of a directly connected network. The interface connected to the specified network will participate in the EIGRP routing process.
mask	(Optional) The network mask for the IP address.

Defaults

No networks are specified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **network** command starts EIGRP on all interfaces with at least one IP address in the specified network. It inserts the connected subnet from the specified network in the EIGRP topology table.

The security appliance then establishes neighbors through the matched interfaces. There is no limit to the number of **network** commands that can be configured on the security appliance.

Examples

The following example defines EIGRP as the routing protocol to be used on all interfaces connected to networks 10.0.0.0 and 192.168.7.0:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 255.0.0.0
hostname(config-router)# network 192.168.7.0 255.255.255.0
```

Related Commands

Command	Description
show eigrp interfaces	Displays information about interfaces configured for EIGRP.
show eigrp topology	Displays the EIGRP topology table.

network-acl

To specify a firewall ACL name that you configured previously using the **access-list** command, use the **network-acl** command in dynamic-access-policy-record configuration mode. To remove an existing network ACL, use the **no** form of this command. To remove all network ACL, use the command without arguments.

network-acl *name*

no network-acl [*name***]**

Syntax Description

name	Specifies the name of the network ACL. Maximum 240 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dynamic-access-policy-record configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use this command multiple time to assign multiple firewall ACLs to the DAP record.

The security appliance verifies each of the ACLs you specify to make sure they contain only permit rules or only deny rules for the access-list entries. If any of the specified ACLs contain mixed permit and deny rules, then the security appliance rejects the command.

The following example shows how to apply a network ACL called Finance Restrictions to the DAP record named Finance.

```
hostname(config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# network-acl Finance Restrictions
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
access-policy	Configures a firewall access policy.

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name***]**	Displays the running configuration for all DAP records, or for the named DAP record.

network area

To define the interfaces on which OSPF runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for interfaces defined with the address/netmask pair, use the **no** form of this command.

network *addr mask* **area** *area_id*

no network *addr mask* **area** *area_id*

Syntax Description

addr	IP address.
area *area_id*	Specifies the area that is to be associated with the OSPF address range. The *area_id* can be specified in either IP address format or in decimal format. When specified in decimal format, valid values range from 0 to 4294967295.
mask	The network mask.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For OSPF to operate on the interface, the address of the interface must be covered by the **network area** command. If the **network area** command does not cover the IP address of the interface, it will not enable OSPF over that interface.

There is no limit to the number of **network area** commands you can use on the security appliance.

Examples

The following example enables OSPF on the 192.168.1.1 interface and assigns it to area 2:

```
hostname(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

network-object

To add a network object to a network object group, use the **network-object** command in network configuration mode. To remove network objects, use the **no** form of this command.

network-object host *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

Syntax Description

host_addr	Host IP address (if the host name is not already defined using the **name** command).
host_name	Host name (if the host name is defined using the **name** command.
net_addr	Network address; used with *netmask* to define a subnet object.
netmask	Netmask; used with *net_addr* to define a subnet object.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Network configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **network-object** command is used with the **object-group** command to define a host or a subnet object in network configuration mode.

Examples

The following example shows how to use the **network-object** command in network configuration mode to create a new network object group:

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
```

```
hostname(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
group-object	Adds network object groups.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

nt-auth-domain-controller

To specify the name of the NT Primary Domain Controller for this server, use the **nt-auth-domain-controller** command in aaa-server host configuration mode. To remove this specification, use the **no** form of this command:

nt-auth-domain-controller *string*

no nt-auth-domain-controller

Syntax Description

string	Specify the name, up to 16 characters long, of the Primary Domain Controller for this server.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid only for NT Authentication AAA servers. You must have first used the **aaa-server host** command to enter host configuration mode. The name in the *string* variable must match the NT entry on the server itself.

Examples

The following example configures the name of the NT Primary Domain Controller for this server as "primary1".

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.

clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

ntp authenticate

To enable authentication with an NTP server, use the **ntp authenticate** command in global configuration mode. To disable NTP authentication, use the **no** form of this command.

ntp authenticate

no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you enable authentication, the security appliance only communicates with an NTP server if it uses the correct trusted key in the packets (see the **ntp trusted-key** command). The security appliance also uses an authentication key to synchronize with the NTP server (see the **ntp authentication-key** command).

Examples

The following example configures the security appliance to synchronize only to systems that provide authentication key 42 in their NTP packets:

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

Related Commands

Command	Description
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.

Command	Description
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

ntp authentication-key

To set a key to authenticate with an NTP server, use the **ntp authentication-key** command in global configuration mode. To remove the key, use the **no** form of this command.

ntp authentication-key *key_id* **md5** *key*

no ntp authentication-key *key_id* [**md5** *key*]

Syntax Description

key_id	Identifies a key ID between 1 and 4294967295. You must specify this ID as a trusted key using the **ntp trusted-key** command.
md5	Specifies the authentication algorithm as MD5, which is the only algorithm supported.
key	Sets the key value as a string up to 32 characters in length.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To use NTP authentication, also configure the **ntp authenticate** command.

Examples

The following example enables authentications, identifies trusted key IDs 1 and 2, and sets authentication keys for each trusted key ID:

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

ntp server

To identify an NTP server to set the time on the security appliance, use the **ntp server** command in global configuration mode. To remove the server, use the **no** form of this command. You can identify multiple servers; the security appliance uses the most accurate server. In multiple context mode, set the NTP server in the system configuration only.

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

Syntax Description

ip_address	Sets the IP address of the NTP server.
key *key_id*	If you enable authentication using the **ntp authenticate** command, sets the trusted key ID for this server. See also the **ntp trusted-key** command.
source *interface_name*	Identifies the outgoing interface for NTP packets if you do not want to use the default interface in the routing table. Because the system does not include any interfaces in multiple context mode, specify an interface name defined in the admin context.
prefer	Sets this NTP server as the preferred server if multiple servers have similar accuracy. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the **prefer** keyword specifies which of those servers to use. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. For example, the security appliance uses a server of stratum 2 over a server of stratum 3 that is preferred.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to make the source interface optional.

Examples

The following example identifies two NTP servers and enables authentication for the key IDs 1 and 2:

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
```

```
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

ntp trusted-key

To specify an authentication key ID to be a trusted key, which is required for authentication with an NTP server, use the **ntp trusted-key** command in global configuration mode. To remove the trusted key, use the **no** form of this command. You can enter multiple trusted keys for use with multiple servers.

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

Syntax Description

key_id	Sets a key ID between 1 and 4294967295.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To use NTP authentication, also configure the **ntp authenticate** command. To synchronize with a server, set the authentication key for the key ID using the **ntp authentication-key** command.

Examples

The following example enables authentications, identifies trusted key IDs 1 and 2, and sets authentication keys for each trusted key ID:

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.

Command	Description
show ntp associations	Shows the NTP servers with which the security appliance is associated.
show ntp status	Shows the status of the NTP association.

num-packets

To specify the number of request packets sent during an SLA operation, use the **num-packets** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

num-packets *number*

no num-packets *number*

Syntax Description

number	The number of packets sent during an SLA operation. Valid values are from 1 to 100.

Defaults

The default number of packets sent for echo types is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Increase the default number of packets sent to prevent incorrect reachability information due to packet loss.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes and the number of echo requests sent during an SLA operation to 5.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
request-data-size	Specifies the size of the request packet payload.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

object-group

To define object groups that you can use to optimize your configuration, use the **object-group** command in global configuration mode. Use the **no** form of this command to remove object groups from the configuration. This command supports IPv4 and IPv6 addresses.

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* [**tcp | udp | tcp-udp**]

no object-group service *obj_grp_id* [**tcp | udp | tcp-udp**]

Syntax Description

icmp-type	Defines a group of ICMP types such as echo and echo-reply. After entering the main **object-group icmp-type** command, add ICMP objects to the ICMP type group with the **icmp-object** and the **group-object** commands.
network	Defines a group of hosts or subnet IP addresses. After entering the main **object-group network** command, add network objects to the network group with the **network-object** and the **group-object** commands.
obj_grp_id	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.
protocol	Defines a group of protocols such as TCP and UDP. After entering the main **object-group protocol** command, add protocol objects to the protocol group with the **protocol-object** and the **group-object** commands.
service	An enhanced service object group defines a mix of TCP services, UDP services, ICMP-type services, and any protocol if **tcp**, **udp**, or **tcp-udp** is not specified on the command line. After entering the main **object-group service** command, add service objects to the service group with the **service-object** and the **group-object** commands. When **tcp**, **udp**, or **tcp-udp** is optionally specified on the command line, **service** defines a standard service object group of TCP/UDP port specifications such as "eq smtp" and "range 2000 2010." In this case, after entering the main **object-group service** command, add port objects to the service group with the **port-object** and the **group-object** commands.
tcp	Specifies that service group is used for TCP.
tcp-udp	Specifies that service group can be used for TCP and UDP.
udp	Specifies that service group is used for UDP.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.

When you define a group with the **object-group** command and then use any security appliance command, the command applies to every item in that group. This feature can significantly reduce your configuration size.

Once you define an object group, you must use the **object-group** keyword before the group name in all applicable security appliance commands as follows:

```
hostname# show running-config object-group group_name
```

where *group_name* is the name of the group.

This example shows the use of an object group once it is defined:

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

In addition, you can group **access list** command arguments:

Individual Arguments	Object Group Replacement
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

You can group commands hierarchically; an object group can be a member of another object group.

To use object groups, you must do the following:

- Use the **object-group** keyword before the object group name in all commands as follows:

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group locals
  object-group eng_svc
  ```

  where *remotes* and *locals* are sample object group names.
- The object group must be nonempty.
- You cannot remove or empty an object group if it is currently being used in a command.

After you enter a main **object-group** command, the command mode changes to its corresponding mode. The object group is defined in the new mode. The active mode is indicated in the command prompt format. For example, the prompt in the configuration terminal mode appears as follows:

```
hostname(config)#
```

where *hostname* is the name of the security appliance.

However, when you enter the **object-group** command, the prompt appears as follows:

```
hostname(config-type)#
```

where *hostname* is the name of the security appliance, and *type is the object-group type.*

Use the **exit**, **quit**, or any valid config-mode commands such as **access-list** to close an **object-group** mode and exit the **object-group** main command.

The **show running-config object-group** command displays all defined object groups by their *grp_id* when the **show running-config object-group** *grp_id* command is entered, and by their group type when you enter the **show running-config object-group** *grp_type* command. When you enter the **show running-config object-group** command without an argument, all defined object groups are shown.

Use the **clear configure object-group** command to remove a group of previously defined **object-group** commands. Without an argument, the **clear configure object-group** command lets you to remove all defined object groups that are not being used in a command. The *grp_type* argument removes all defined object groups that are not being used in a command for that group type only.

You can use all other security appliance commands in an object-group mode, including the **show running-config** and **clear configure** commands.

Commands within the object-group mode appear indented when displayed or saved by the **show running-config object-group**, **write**, or **config** commands.

Commands within the object-group mode have the same command privilege level as the main command.

When you use more than one object group in an **access-list** command, the elements of all object groups that are used in the command are linked together, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

The starting position of the description text is the character right after the white space (a blank or a tab) following the **description** keyword.

Examples

The following example shows how to use the **object-group icmp-type** mode to create a new icmp-type object group:

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

The following example shows how to use the **object-group network** command to create a new network object group:

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

The following example shows how to use the **object-group network** command to create a new network object group and map it to an existing object-group:

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

The following example shows how to use the **object-group protocol** mode to create a new protocol object group:

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

The following example shows how to use the **object-group service** mode to create a new port (service) object group:

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

The following example shows how to add and remove a text description to an object group:

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

The following example shows how to use the **group-object** mode to create a new object group that consists of previously defined objects:

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit

hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

Without the **group-object** command, you need to define the *all_hosts* group to include all the IP addresses that have already been defined in *host_grp_1* and *host_grp_2*. With the **group-object** command, the duplicated definitions of the hosts are eliminated.

The following examples show how to use object groups to simplify the access list configuration:

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 172.23.56.10
hostname(config-network)# network-object host 172.23.56.20
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object host 172.23.56.195

hostname(config)# object-group service eng_svc ftp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

This grouping enables the access list to be configured in 1 line instead of 24 lines, which would be needed if no grouping is used. Instead, with the grouping, the access list configuration is as follows:

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

Note The **show running-config object-group** and **write** commands allow you to display the access list as configured with the object group names. The **show access-list** command displays the access list entries that are expanded out into individual entries without their object groupings.

Related Commands

Command	Description
clear configure object-group	Removes all the **object group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

ocsp disable-nonce

To disable the nonce extension, use the **ocsp disable-nonce** command in crypto ca trustpoint configuration mode. By default, OCSP requests include a nonce extension, which cryptographically binds requests with responses to avoid replay attacks. However, some OCSP servers use pre-generated responses that do not contain this matching nonce extension. To use OCSP with these servers, you must disable the nonce extension. To re-enable the nonce extension, use the **no** form of this command.

ocsp disable-nonce

no ocsp disable-nonce

Syntax Description

This command has no keywords or arguments.

Defaults

By default, OCSP requests include a nonce extension.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When you use this command, the OCSP request does not include the OCSP nonce extension, and the security appliance does not check it.

Examples

The following example shows how to disable the nonce extension for a trustpoint called newtrust.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp disable-nonce
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint mode. Use this command in global configuration mode.
match certificate	Configures an OCSP override rule.

Command	Description
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

ocsp url

To configure an OCSP server for the security appliance to use to check all certificates associated with a trustpoint rather than the server specified in the AIA extension of the client certificate, use the **ocsp url** command in crypto ca trustpoint configuration mode. To remove the server from the configuration, use the **no** form of this command.

ocsp url *URL*

no ocsp url

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance supports only HTTP URLs, and you can specify only one URL per trustpoint.

The security appliance provides three ways to define an OCSP server URL, and it attempts to use OCSP servers according to how you define them, in the following order:

- An OCSP server you set using **match certificate** command.
- An OCSP server you set using the **ocsp url** command.
- The OCSP server in the AIA field of the client certificate.

If you do not configure an OCSP URL via the **match certificate** command or the **ocsp url** command, the security appliance uses the OCSP server in the AIA extension of the client certificate. If the certificate does not have an AIA extension, revocation status checking fails.

Examples

The following example shows how to configure an OCSP server with the URL http://10.1.124.22.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp url http://10.1.124.22
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint mode. Use this command in global configuration mode.
match certificate	Configures an OCSP override rule,
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

onscreen-keyboard

To insert an onscreen keyboard into the logon pane or all panes with a login/password requirement, use the **onscreen-keyboard** command in webvpn mode. To remove a previously configured onscreen keyboard, use the **no** version of the command.

onscreen-keyboard {logon | all}

no onscreen-keyboard [logon | all]

Syntax Description

logon	Inserts the onscreen keyboard for the logon pane.
all	Inserts the onscreen keyboard for the logon pane, and for all other panes with a login/password requirement.

Defaults

No onscreen keyboard.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The onscreen keyboard lets you enter user credentials without keystrokes.

Examples

The following example shows how to enable the onscreen keyboard for the logon page:

```
hostname(config)# webvpn
hostname(config-webvpn)# onscreen-keyboard logon
hostname(config-webvpn)#
```

Related Commands

Command	Description
webvpn	Enters webvpn mode, which lets you configure attributes for clientless SSLVPN connections.

ospf authentication

To enable the use of OSPF authentication, use the **ospf authentication** command in interface configuration mode. To restore the default authentication stance, use the **no** form of this command.

ospf authentication [**message-digest** | **null**]

no ospf authentication

Syntax Description

message-digest	(Optional) Specifies to use OSPF message digest authentication.
null	(Optional) Specifies to not use OSPF authentication.

Defaults

By default, OSPF authentication is not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before using the **ospf authentication** command, configure a password for the interface using the **ospf authentication-key** command. If you use the **message-digest** keyword, configure the message-digest key for the interface with the **ospf message-digest-key** command.

For backward compatibility, authentication type for an area is still supported. If the authentication type is not specified for an interface, the authentication type for the area will be used (the area default is null authentication).

When this command is used without any options, simple password authentication is enabled.

Examples

The following example shows how to enable simple password authentication for OSPF on the selected interface:

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

Related Commands

Command	Description
ospf authentication-key	Specifies the password used by neighboring routing devices.
ospf message-digest-key	Enables MD5 authentication and specifies the MD5 key.

ospf authentication-key

To specify the password used by neighboring routing devices, use the **ospf authentication-key** command in interface configuration mode. To remove the password, use the **no** form of this command.

ospf authentication-key *password*

no ospf authentication-key

Syntax Description<

password	Assigns an OSPF authentication password for use by neighboring routing devices. The password must be less than 9 characters. You can include blank space between two characters. Spaces at the beginning or end of the password are ignored.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The password created by this command is used as a key that is inserted directly into the OSPF header when routing protocol packets are originated. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to exchange OSPF information.

ExamplesNote

The following example shows how to specify a password for OSPF authentication:

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

Related Commands

Command	Description
area authentication	Enables OSPF authentication for the specified area.
ospf authentication	Enables the use of OSPF authentication.

ospf cost

To specify the cost of sending a packet through the interface, use the **ospf cost** command in interface configuration mode. To reset the interface cost to the default value, use the **no** form of this command.

ospf cost *interface_cost*

no ospf cost

Syntax Description

interface_cost	The cost (a link-state metric) of sending a packet through an interface. This is an unsigned integer value from 0 to 65535. 0 represents a network that is directly connected to the interface, and the higher the interface bandwidth, the lower the associated cost to send packets across that interface. In other words, a large cost value represents a low bandwidth interface and a small cost value represents a high bandwidth interface. The OSPF interface default cost on the security appliance is 10. This default differs from Cisco IOS software, where the default cost is 1 for fast Ethernet and Gigabit Ethernet and 10 for 10BaseT. This is important to take into account if you are using ECMP in your network.

Defaults

The default *interface_cost* is 10.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ospf cost** command lets you explicitly specify the cost of sending a packet on an interface. The *interface_cost* parameter is an unsigned integer value from 0 to 65535.

The **no ospf cost** command allows you to reset the path cost to the default value.

Examples

The following example show how to specify the cost of sending a packet on the selected interface:

```
hostname(config-if)# ospf cost 4
```

Related Commands

Command	Description
show running-config interface	Displays the configuration of the specified interface.

ospf database-filter

To filter out all outgoing LSAs to an OSPF interface during synchronization and flooding, use the **ospf database-filter** command in interface configuration mode. To restore the LSAs, use the **no** form of this command.

ospf database-filter all out

no ospf database-filter all out

Syntax Description

all out	Filters all outgoing LSAs to an OSPF interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ospf database-filter** command filters outgoing LSAs to an OSPF interface. The **no ospf database-filter all out** command restores the forwarding of LSAs to the interface.

Examples

The following example shows how to use the **ospf database-filter** command to filter outgoing LSAs:

```
hostname(config-if)# ospf database-filter all out
```

Related Commands

Command	Description
show interface	Displays interface status information.

ospf dead-interval

To specify the interval before neighbors declare a router down, use the **ospf dead-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf dead-interval *seconds*

no ospf dead-interval

Syntax Description

seconds	The length of time during which no hello packets are seen. The default for *seconds* is four times the interval set by the **ospf hello-interval** command (which ranges from 1 to 65535).

Defaults

The default value for *seconds* is four times the interval set by the **ospf hello-interval** command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ospf dead-interval** command lets you set the dead interval before neighbors to declare the router down (the length of time during which no hello packets are seen). The *seconds* argument specifies the dead interval and must be the same for all nodes on the network. The default for *seconds* is four times the interval set by the **ospf hello-interval** command from 1 to 65535.

The **no ospf dead-interval** command lets restores the default interval value.

Examples

The following example sets the OSPF dead interval to 1 minute:

```
hostname(config-if)# ospf dead-interval 60
```

Related Commands

Command	Description
ospf hello-interval	Specifies the interval between hello packets sent on an interface.
show ospf interface	Displays OSPF-related interface information.

ospf hello-interval

To specify the interval between hello packets sent on an interface, use the **ospf hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

ospf hello-interval *seconds*

no ospf hello-interval

Syntax Description

seconds	Specifies the interval between hello packets that are sent on the interface; valid values are from 1 to 65535 seconds.

Defaults

The default value for **hello-interval** *seconds* is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This value is advertised in the hello packets. The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Examples

The following example sets the OSPF hello interval to 5 seconds:

```
hostname(config-if)# ospf hello-interval 5
```

Related Commands

Command	Description
ospf dead-interval	Specifies the interval before neighbors declare a router down.
show ospf interface	Displays OSPF-related interface information.

ospf message-digest-key

To enable OSPF MD5 authentication, use the **ospf message-digest-key** command in interface configuration mode. To remove an MD5 key, use the **no** form of this command.

ospf message-digest-key *key-id* **md5** *key*

no ospf message-digest-key

Syntax Description

key-id	Enables MD5 authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
md5 *key*	Alphanumeric password of up to 16 bytes. You can include spaces between key characters. Spaces at the beginning or end of the key are ignored. MD5 authentication verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ospf message-digest-key** command lets you enable MD5 authentication. The **no** form of the command let you remove an old MD5 key. *key_id* is a numerical identifier from 1 to 255 for the authentication key. *key* is an alphanumeric password of up to 16 bytes. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

Examples

The following example shows how to specify an MD5 key for OSPF authentication:

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

Related Commands

Command	Description
area authentication	Enables OSPF area authentication.
ospf authentication	Enables the use of OSPF authentication.

ospf mtu-ignore

To disable OSPF maximum transmission unit (MTU) mismatch detection on receiving database packets, use the **ospf mtu-ignore** command in interface configuration mode. To restore MTU mismatch detection, use the **no** form of this command.

ospf mtu-ignore

no ospf mtu-ignore

Syntax Description

This command has no arguments or keywords.

Defaults

By default, **ospf mtu-ignore** is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange Database Descriptor (DBD) packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.The **ospf mtu-ignore** command disables OSPF MTU mismatch detection on receiving DBD packets. It is enabled by default.

Examples

The following example shows how to disable the **ospf mtu-ignore** command:

```
hostname(config-if)# ospf mtu-ignore
```

Related Commands

Command	Description
show interface	Displays interface status information.

ospf network point-to-point non-broadcast

To configure the OSPF interface as a point-to-point, non-broadcast network, use the **ospf network point-to-point non-broadcast** command in interface configuration mode. To remove this command from the configuration, use the **no** form of this command. The **ospf network point-to-point non-broadcast** command lets you to transmit OSPF routes over VPN tunnels.

ospf network point-to-point non-broadcast

no ospf network point-to-point non-broadcast

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When the interface is specified as point-to-point, the OSPF neighbors have to be manually configured; dynamic discovery is not possible. To manually configure OSPF neighbors, use the **neighbor** command in router configuration mode.

When an interface is configured as point-to-point, the following restrictions apply:

- You can define only one neighbor for the interface.
- You need to define a static route pointing to the crypto endpoint.
- The interface cannot form adjacencies unless neighbors are configured explicitly.
- If OSPF over the tunnel is running on the interface, regular OSPF with an upstream router cannot be run on the same interface.
- You should bind the crypto-map to the interface before specifying the OSPF neighbor to ensure that the OSPF updates are passed through the VPN tunnel. If you bind the crypto-map to the interface after specifying the OSPF neighbor, use the **clear local-host all** command to clear OSPF connections so the OSPF adjacencies can be established over the VPN tunnel.

Examples

The following example shows how to configure the selected interface as a point-to-point, non-broadcast interface:

```
hostname(config-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

Related Commands

Command	Description
neighbor	Specifies manually configured OSPF neighbors.
show interface	Displays interface status information.

ospf priority

To change the OSPF router priority, use the **ospf priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

ospf priority *number*

no ospf priority [*number*]

Syntax Description

number	Specifies the priority of the router; valid values are from 0 to 255.

Defaults

The default value for *number* is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When two routers attached to a network both attempt to become the designated router, the one with the higher router priority takes precedence. If there is a tie, the router with the higher router ID takes precedence. A router with a router priority set to zero is ineligible to become the designated router or backup designated router. Router priority is configured only for interfaces to multiaccess networks (in other words, not to point-to-point networks).

Examples

The following example shows how to change the OSPF priority on the selected interface:

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

ospf retransmit-interval

To specify the time between LSA retransmissions for adjacencies belonging to the interface, use the **ospf retransmit-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

Syntax Description

seconds	Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.

Defaults

The default value of **retransmit-interval** *seconds* is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgment message. If the router receives no acknowledgment, it will re-send the LSA.

The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines and virtual links.

Examples

The following example shows how to change the retransmit interval for LSAs:

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

ospf transmit-delay

To set the estimated time required to send a link-state update packet on the interface, use the **ospf transmit-delay** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

Syntax Description

seconds	Sets the estimated time required to send a link-state update packet on the interface. The default value is 1 second with a range from 1 to 65535 seconds.

Defaults

The default value of *seconds* is 1 second.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

LSAs in the update packet must have their ages incremented by the amount specified in the *seconds* argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low-speed links.

Examples

The following example sets the transmit delay to 3 seconds for the selected interface:

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.

otp expiration

To specify the duration in hours that an issued One-Time Password (OTP) for the local Certificate Authority (CA) enrollment page is valid, use the **otp expiration** command in CA server configuration mode. To reset the duration to the default number of hours, use the **no** form of this command.

otp expiration *timeout*

no otp expiration

Syntax Description

timeout	Specifies the time in hours users have to enroll for a certificate from the local CA before the OTP for the enrollment page expires. Valid values range from 1 to 720 hours (30 days).

Defaults

By default, a OTP expiration for certificate enrollment is 72 hours (3 days).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The OTP expiration period specifies the number of hours that a user has to login to the enrollment page of the CA server. Once the user logs in and enrolls for a certificate, the time period specified by the **enrollment retrieval** command starts.

Note The user OTP for enrolling for a certificate with the enrollment interface page is also used as the password to unlock the PKCS12 file containing that user's issued certificate and keypair.

Examples

The following example specifies that the OTP for the enrollment page applies for 24 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# otp expiration 24
hostname(config-ca-server)#
```

The following example resets the OTP duration to the default of 72 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server))# no otp expiration
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
enrollment-retrieval	Specifies the time in hours that an enrolled user can retrieve a PKCS12 enrollment file.
show crypto ca server	Displays the certificate authority configuration.

outstanding

To limit the number of unauthenticated e-mail proxy sessions, use the **outstanding** command in the applicable e-mail proxy configuration mode. To remove the attribute from the configuration, use the **no** version of this command.

outstanding {*number*}

no outstanding

Syntax Description

number	The number of unauthenticated sessions permitted. The range is from 1 to 1000.

Defaults

The default is 20.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **no** version of this command to remove the attribute from the configuration, which permits an unlimited number of unauthenticated sessions. This also limit s DOS attacks on the e-mail ports.

E-mail proxy connections have three states:

1. A new e-mail connection enters the “unauthenticated” state.
2. When the connection presents a username, it enters the “authenticating” state.
3. When the security appliance authenticates the connection, it enters the “authenticated” state.

If the number of connections in the unauthenticated state exceeds the configured limit, the security appliance terminates the oldest unauthenticated connection, preventing overload. It does not terminate authenticated connections.

Examples

The following example shows how to set a limit of 12 unauthenticated sessions for POP3S e-mail proxy.

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

override-account-disable

To override an account-disabled indication from a AAA server, use the **override-account-disable** command in tunnel-group general-attributes configuration mode. To disable an override, use the **no** form of this command.

override-account-disable

no override-account-disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

This command is valid for servers, such as RADIUS with NT LDAP, and Kerberos, that return an "account-disabled" indication.

You can configure this attribute for IPSec RA and WebVPN tunnel-groups.

Examples

The following example allows overriding the "account-disabled" indicator from the AAA server for the WebVPN tunnel group "testgroup":

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

The following example allows overriding the "account-disabled" indicator from the AAA server for the IPSec remote access tunnel group "QAgroup":

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the tunnel-group database or the configuration for a particular tunnel group.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

override-svc-download

To configure the connection profile to override the group policy or username attributes configuration for downloading an AnyConnect or SSL VPN client, use the **override-svc-download** command from tunnel-group webvpn attributes configuration mode. To remove the command from the configuration, use the **no** form of the command:

override-svc-download enable

no override-svc-download enable

Defaults

The default is disabled. The security appliance does not override the group policy or username attributes configuration for downloading the client.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance allows clientless, AnyConnect, or SSL VPN client connections for remote users based on whether clientless and/or SSL VPN is enabled in the group policy or username attributes with the **vpn-tunnel-protocol** command. The **svc ask** command further modifies the client user experience by prompting the user to download the client or return to the WebVPN home page.

However, you may want clientless users logging in under specific tunnel groups to not experience delays waiting for the download prompt to expire before being presented with the clientless SSL VPN home page. You can prevent delays for these users at the connection profile level with the **override-svc-download** command. This command causes users logging through a connection profile to be immediately presented with the clientless SSL VPN home page regardless of the **vpn-tunnel-protocol** or **svc ask** command settings.

Examples

In the following example, the user enters tunnel-group webvpn attributes configuration mode for the connection profile *engineering* and enables the connection profile to override the group policy and username attribute settings for client download prompts:

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# override-svc-download
```

Related Commands

Command	Description
show webvpn svc	Displays information about installed SSL VPN clients.
svc	Enables or requires the SSL VPN client for a specific group or user.
svc image	Specifies a client package file that the security appliance expands in cache memory for downloading to remote PCs.

CHAPTER 22

packet-tracer through pwd Commands

packet-tracer

To enable packet tracing capabilities for packet sniffing and network fault isolation, use the **packet-tracer** commandin privileged EXEC configuration mode. To disable packet capture capabilities, use the **no** form of this command.

packet-tracer input [*src_int*] *protocol src_addr src_port dest_addr dest_port* [**detailed**] [**xml**]

no packet-tracer

Syntax Description

input *src_int*	Specifies the source interface for the packet trace.
protocol	Specifies the protocol type for the packet trace. Available protocol type keywords are *icmp*, *rawip*, *tcp* or *udp*.
src_addr	Specifies the source address for the packet trace.
src_port	Specifies the source port for the packet trace.
dest_addr	Specifies the destination address for the packet trace.
dest_port	Specifies the destination port for the packet trace.
detailed	(Optional) Provides detailed packet trace information.
xml	(Optional) Displays the trace capture in XML format.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Priveleged EXEC mode	•	—	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In addition to capturing packets, it is possible to trace the lifespan of a packet through the security appliance to see if it is behaving as expected. The **packet-tracer** command lets you do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines which caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. In the instance that a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. For example if a packet was dropped because of an invalid header validation, a message is displayed that says, "packet dropped due to bad ip header (reason)."

Examples

To enable packet tracing from inside host 10.2.25.3 to external host 209.165.202.158 with detailed information, enter the following:

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.

page style

To customize the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **page style** command in webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

page style *value*

[**no**] **page style** *value*

Syntax Description

value	Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default page style is background-color:white;font-family:Arial,Helv,sans-serif

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the page style to large:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
title	Customizes the title of the WebVPN page

pager

To set the default number of lines on a page before the "---more---" prompt appears for Telnet sessions, use the **pager** command in global configuration mode.

pager [lines] *lines*

Syntax Description

[**lines**] *lines*	Sets the number of lines on a page before the "---more---" prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Defaults

The default is 24 lines.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from a privileged EXEC mode command to a global configuration mode command. The **terminal pager** command was added as the privileged EXEC mode command.

Usage Guidelines

This command changes the default pager line setting for Telnet sessions. If you want to temporarily change the setting only for the current session, use the **terminal pager** command.

If you Telnet to the admin context, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

Examples

The following example changes the number of lines displayed to 20:

```
hostname(config)# pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messsages to display on the Telnet session.
terminal pager	Sets the number of lines to display in a Telnet session before the "`---more---`" prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

parameters

To enter parameters configuration mode to set parameters for an inspection policy map, use the **parameters** command in policy-map configuration mode.

parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

An inspection policy map may support one or more **parameters** commands. Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

Examples

The following example shows how to set the maximum message length for DNS packets in the default inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

participate

To force the device to participate in the virtual load-balancing cluster, use the **participate** command in VPN load-balancing configuration mode. To remove a device from participation in the cluster, use the **no** form of this command.

participate

no participate

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is that the device does not participate in the vpn load-balancing cluster.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
VPN load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first configure the interface using the **interface** and **nameif** commands, and use the **vpn load-balancing** command to enter VPN load-balancing mode. You must also have previously configured the cluster IP address using the **cluster ip** command and configured the interface to which the virtual cluster IP address refers.

This command forces this device to participate in the virtual load-balancing cluster. You must explicitly issue this command to enable participation for a device.

All devices that participate in a cluster must share the same cluster-specific values: ip address, encryption settings, encryption key, and port.

Note When using encryption, you must have previously configured the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If isakmp is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.

If isakmp was enabled when you configured the **cluster encryption** command, but was disabled before you configured the **participate** command, you get an error message when you enter the **participate** command, and the local device will not participate in the cluster.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **participate** command that enables the current device to participate in the vpn load-balancing cluster:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

passive-interface

To disable the transmission of RIP routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable RIP routing updates on an interface, use the **no** form of this command.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) Sets the specified interface to passive mode.

Defaults

All interfaces are enabled for active RIP when RIP is enabled.

If an interface or the **default** keyword is not specified, the commands defaults to **default** and appears in the configuration as `passive-interface default`.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables but does not broadcast routing updates.

Examples

The following example sets the outside interface to passive RIP. The other interfaces on the security appliance send and receive RIP updates.

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.
router rip	Enables the RIP routing process and enters RIP router configuration mode.
show running-config rip	Displays the RIP commands in the running configuration.

passive-interface (EIGRP)

To disable the sending and receiving of EIGRP routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable routing updates on an interface, use the **no** form of this command.

passive-interface {**default** | *if_name*}

no passive-interface {**default** | *if_name*}

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) The name of the interface, as specified by the **nameif** command, to passive mode.

Defaults

All interfaces are enabled for active routing (sending and receiving routing updates) when routing is enabled for that interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Support for EIGRP routing was added.

Usage Guidelines

Enables passive routing on the interface. For EIGRP, this disables the transmission and reception of routing updates on that interface.

You can have more than one **passive-interface** command in the EIGRP configuration. You can use the **passive-interface default** command to disable EIGRP routing on all interfaces, and then use the **no passive-interface** command to enable EIGRP routing on specific interfaces.

Examples

The following example sets the outside interface to passive EIGRP. The other interfaces on the security appliance send and receive EIGRP updates.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

The following example sets all interfaces except the inside interface to passive EIGRP. Only the inside interface will send and receive EIGRP updates.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface default
hostname(config-router)# no passive-interface inside
```

Related Commands

Command	Description
show running-config router	Displays the router configuration commands in the running configuration.

passwd

To set the login password, use the **passwd** command in global configuration mode. To set the password back to the default of "cisco," use the **no** form of this command. You are prompted for the login password when you access the CLI as the default user using Telnet or SSH. After you enter the login password, you are in user EXEC mode.

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **passwd** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.
passwd | **password**	You can enter either command; they are aliased to each other.
password	Sets the password as a case-sensitive string of up to 80 characters. The password must not contains spaces.

Defaults

The default password is "cisco."

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This login password is for the default user. If you configure CLI authentication per user for Telnet or SSH using the **aaa authentication console** command, then this password is not used.

Examples

The following example sets the password to Pa$$w0rd:

```
hostname(config)# passwd Pa$$w0rd
```

The following example sets the password to an encrypted password that you copied from another security appliance:

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

password (crypto ca trustpoint)

To specify a challenge phrase that is registered with the CA during enrollment, use the **password** command in crypto ca trustpoint configuration mode. The CA typically uses this phrase to authenticate a subsequent revocation request. To restore the default setting, use the **no** form of the command.

password *string*

no password

Syntax Description

string	Specifies the name of the password as a character string. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, “hello 21” is a legal password, but “21 hello” is not. The password checking is case sensitive. For example, the password “Secret” is different from the password “secret”.

Defaults

The default setting is to not include a password.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command lets you specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the security appliance.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes a challenge phrase registered with the CA in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

password-management

To enable password management, use the **password-management** command in tunnel-group general-attributes configuration mode. To disable password management, use the **no** form of this command. To reset the number of days to the default value, use the **no** form of the command with the **password-expire-in-days** keyword specified.

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

Syntax Description

days	Specifies the number of days (0 through 180) before the current password expires. This parameter is required if you specify the **password-expire-in-days** keyword.
password-expire-in-days	(Optional) Indicates that the immediately following parameter specifies the number of days before the current password expires that the security appliance starts warning the user about the pending expiration. This option is valid only for LDAP servers. See the Usage Notes section for more information.

Defaults

If you do not specify this command, no password management occurs. If you do not specify the **password-expire-in-days** keyword, the default length of time to start warning before the current password expires is 14 days.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The security appliance supports password management for the RADIUS and LDAP protocols. It supports the “password-expire-in-days” option for LDAP only.

You can configure password management for IPSec remote access and SSL VPN tunnel-groups.

When you configure the password-management command, the security appliance notifies the remote user at login that the user's current password is about to expire or has expired. The security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password.

This command is valid for AAA servers that support such notification. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note Some RADIUS servers that support MSCHAP currently do not support MSCHAPv2. This command requires MSCHAPv2 so please check with your vendor.

The security appliance, releases 7.1 and later, generally supports password management for the following connection types when authenticating with LDAP or with any RADIUS configuration that supports MS-CHAPv2:

- AnyConnect VPN Client
- IPSec VPN Client
- Clientless SSL VPN

Password management is *not* supported for any of these connection types for Kerberos/Active Directory (Windows password) or NT 4.0 Domain. The RADIUS server (for example, Cisco ACS) could proxy the authentication request to another authentication server. However, from the security appliance perspective, it is talking only to a RADIUS server.

Note For LDAP, the method to change a password is proprietary for the different LDAP servers on the market. Currently, the security appliance implements the proprietary password management logic only for Microsoft Active Directory and Sun LDAP servers.

Native LDAP requires an SSL connection. You must enable LDAP over SSL before attempting to do password management for LDAP. By default, LDAP uses port 636.

Note that this command does not change the number of days before the password expires, but rather, the number of days ahead of expiration that the security appliance starts warning the user that the password is about to expire.

If you do specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The security appliance does not notify the user of the pending expiration, but the user can change the password after it expires.

Examples

The following example sets the days before password expiration to begin warning the user of the pending expiration to 90 for the WebVPN tunnel group "testgroup":

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

The following example uses the default value of 14 days before password expiration to begin warning the user of the pending expiration for the IPSec remote access tunnel group "QAgroup":

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
passwd	Sets the login password.
radius-with-expiry	Enables negotiation of password update during RADIUS authentication (Deprecated).
show running-config passwd	Shows the login password in encrypted form.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

password-parameter

To specify the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication, use the **password-parameter** command in aaa-server- host configuration mode. This is an SSO with HTTP Forms command.

password-parameter *string*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The name of the password parameter included in the HTTP POST request. The maximum password length is 128 characters.

Defaults

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The required command **password-parameter** specifies that the POST request must include a user password parameter for SSO authentication.

Note At login, the user enters the actual password value which is entered into the POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies a password parameter named user_password:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
start-url	Specifies the URL at which to retrieve a pre-login cookie.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

password-prompt

To customize the password prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **password-prompt** command from webvpn customization mode:

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text of the password prompt is “PASSWORD:”.

The default style of the password prompt is color:black;font-weight:bold;text-align:right.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to “Corporate Password:”, and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# password-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# password-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page
username-prompt	Customizes the username prompt of the WebVPN page

password-storage

To let users store their login passwords on the client system, use the **password-storage enable** command in group-policy configuration mode or username configuration mode. To disable password storage, use the **password-storage disable** command.

To remove the password-storage attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for password-storage from another group policy.

password-storage {enable | disable}

no password-storage

Syntax Description

disable	Disables password storage.
enable	Enables password storage.

Defaults

Password storage is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Enable password storage only on systems that you know to be in secure sites.

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

Examples

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

To specify whether to validate the identity of the peer using the peer's certificate, use the **peer-id-validate** command in tunnel-group ipsec-attributes mode. To return to the default value, use the **no** form of this command.

peer-id-validate *option*

no peer-id-validate

Syntax Description

option	Specifies one of the following options: • **req**: required • **cert**: if supported by certificate • **nocheck**: do not check

Defaults

The default setting for this command is **req**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec attributes	•	—	•	—	—

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPSec tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, requires validating the peer using the identity of the peer's certificate for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

perfmon

To display performance information, use the **perfmon** command in privileged EXEC mode.

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

Syntax Description

verbose	Displays performance monitor information at the security appliance console.
interval *seconds*	Specifies the number of seconds before the performance display is refreshed on the console.
quiet	Disables the performance monitor displays.
settings	Displays the interval and whether it is quiet or verbose.
detail	Displays detailed information about performance.

Defaults

The *seconds* is 120 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0	Support for this command was introduced on the security appliance.
7.2(1)	Support for the **detail** keyword was added.

Usage Guidelines

The **perfmon** command allows you to monitor the performance of the security appliance. Use the **show perfmon** command to display the information immediately. Use the **perfmon verbose** command to display the information every 2 minutes continuously. Use the **perfmon interval** *seconds* command with the **perfmon verbose** command to display the information continuously every number of seconds that you specify.

An example of the performance information is displayed as follows:

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s

FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

This information lists the number of translations, connections, Websense requests, address translations (called “fixups”), and AAA transactions that occur each second.

Examples

This example shows how to display the performance monitor statistics every 30 seconds on the security appliance console:

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

Command	Description
show perfmon	Displays performance information.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To disable, use the **no** form of this command.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

Syntax Description

days-of-the-week	(Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Defaults

If a value is not entered with the **periodic** command, access to the security appliance as defined with the **time-range** command is in effect immediately and always on.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.

Examples

Some examples follow:

If you want:	Enter this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekdays 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight	**periodic weekend 12:00 to 23:59**

The following example shows how to allow access to the security appliance on Monday through Friday, 8:00 a.m. to 6:00 p.m. only:

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

The following example shows how to allow access to the security appliance on specific days (Monday, Tuesday, and Friday), 10:30 a.m. to 12:30 p.m.:

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the security appliance.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
time-range	Defines access control to the security appliance based on time.

permit errors

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, use the **permit errors** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. To return to the default behavior, where all invalid packets or packets that failed, during parsing, are dropped. use the **no** form of this command.

permit errors

no permit errors

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all invalid packets or packets that failed, during parsing, are dropped.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **permit errors** command in GTP map configuration mode to allow any packets that are invalid or encountered an error during inspection of the message to be sent through the security appliance instead of being dropped.

Examples

The following example permits traffic containing invalid packets or packets that failed, during parsing:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.

Commands	Description
permit response	Supports load-balancing GSNs.
show service-policy inspect gtp	Displays the GTP configuration.

permit response

To support load-balancing GSNs, use the **permit response** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to allow the security appliance to drop GTP responses from GSNs other than the host to which the request was sent.

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

Syntax Description

from-object-group *from_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can send responses to the set of GSNs in the object-group specified by the *to_obj_group_id* argument. The security appliance supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.
to-object-group *to_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can receive responses from the set of GSNs in the object-group specified by the *from_obj_group_id* argument. The security appliance supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.

Defaults

By default, the security appliance drops GTP responses from GSNs other than the host to which the request was sent.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

Use the **permit response** command in GTP map configuration mode to support load-balancing GSNs. The **permit response** command configures the GTP map to allow GTP responses from a different GSN than the response was sent to.

You identify the pool of load-balancing GSNs as a network object. Likewise, you identify the SGSN as a network object. If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in a object group that the responding GSN is permitted to send a GTP response to, the security appliance permits the response.

Examples

The following example permits GTP responses from any host on the 192.168.32.0 network to the host with the IP address 192.168.112.57:

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
permit errors	Allow invalid GTP packets.
show service-policy inspect gtp	Displays the GTP configuration.

pfs

To enable PFS, use the **pfs enable** command in group-policy configuration mode. To disable PFS, use the **pfs disable** command. To remove the PFS attribute from the running configuration, use the **no** form of this command.

pfs {enable | disable}

no pfs

Syntax Description

disable	Disables PFS.
enable	Enables PFS.

Defaults

PFS is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PFS setting on the VPN Client and the security appliance must match.

use the **no** form of this command to allow the inheritance of a value for PFS from another group policy.

In IPSec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.

Examples

The following example shows how to set PFS for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

phone-proxy

To configure the Phone Proxy instance, use the **phone-proxy** command in global configuration mode. To remove the Phone Proxy instance, use the **no** form of this command.

phone-proxy *phone_proxy_name*

no phone-proxy *phone_proxy_name*

Syntax Description

phone_proxy_name	Specifies the name of the Phone Proxy instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Only one Phone Proxy instance can be configured on the security appliance.

If NAT is configured for the HTTP proxy server, the global or mapped IP address of the HTTP proxy server with respect to the IP phones is written to the Phone Proxy configuration file.

Examples

The following example shows the use of the **phone-proxy** command to configure the Phone Proxy instance:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
hostname(config-phone-proxy)# media-termination address 128.106.254.3
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
hostname(config-phone-proxy)# timeout secure-phones 00:05:00
hostname(config-phone-proxy)# disable service-settings
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
tls-proxy	Configures the TLS proxy instance.

pim

To re-enable PIM on an interface, use the **pim** command in interface configuration mode. To disable PIM, use the **no** form of this command.

pim

no pim

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM on all interfaces by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **multicast-routing** command enables PIM on all interfaces by default. Only the **no** form of the **pim** command is saved in the configuration.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

Examples

The following example disables PIM on the selected interface:

```
hostname(config-if)# no pim
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim accept-register

To configure the security appliance to filter PIM register messages, use the **pim accept-register** command in global configuration mode. To remove the filtering, use the **no** form of this command.

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

Syntax Description

list *acl*	Specifies an access list name or number. Use only extended host ACLs with this command.
route-map *map-name*	Specifies a route-map name. Use extended host ACLs in the referenced route-map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the security appliance will immediately send back a register-stop message.

Examples

The following example restricts PIM register messages to those from sources defined in the access list named “no-ssm-range”:

```
hostname(config)# pim accept-register list no-ssm-range
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim bidir-neighbor-filter

To control which bidir-capable neighbors can participate in the DF election, use the **pim bidir-neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. The access list defines the neighbors that can participate in bidir DF elections. Use only standard ACLs with this command; extended ACLs are not supported.

Defaults

All routers are considered to be bidir capable.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The **pim bidir-neighbor-filter** command enables the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in DF election while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When the **pim bidir-neighbor-filter** command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election does not occur.
- If a denied neighbor supports bidir, then DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Examples

The following example allows 10.1.1.1 to become a PIM bidir neighbor:

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

Command	Description
multicast boundary	Defines a multicast boundary for administratively-scoped multicast addresses.
multicast-routing	Enables multicast routing on the security appliance.

pim dr-priority

To configure the neighbor priority on the security appliance used for designated router election, use the **pim dr-priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

pim dr-priority *number*

no pim dr-priority

Syntax Description

number	A number from 0 to 4294967294. This number is used to determine the priority of the device when determining the designated router. Specifying 0 prevents the security appliance from becoming the designated router.

Defaults

The default value is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The device with the largest priority value on an interface becomes the PIM designated router. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the DR. If a device does not include the DR-Priority Option in hello messages, it is regarded as the highest-priority device and becomes the designated router. If multiple devices do not include this option in their hello messages, then the device with the highest IP address becomes the designated router.

Examples

The following example sets the DR priority for the interface to 5:

```
hostname(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim hello-interval

To configure the frequency of the PIM hello messages, use the **pim hello-interval** command in interface configuration mode. To restore the hello-interval to the default value, use the **no** form of this command.

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the security appliance waits before sending a hello message. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.

Defaults

30 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the PIM hello interval to 1 minute:

```
hostname(config-if)# pim hello-interval 60
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim join-prune-interval

To configure the PIM join/prune interval, use the **pim join-prune-interval** command in interface configuration mode. To restore the interval to the default value, use the **no** form of this command.

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the security appliance waits before sending a join/prune message. Valid values range from 10 to 600 seconds. 60 seconds is the default.

Defaults

60 seconds

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the PIM join/prune interval to 2 minutes:

```
hostname(config-if)# pim join-prune-interval 120
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim neighbor-filter

To control which neighbor routers can participate in PIM, use the **pim neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. Use only standard ACLs with this command; extended ACLs are not supported.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command defines which neighbor routers can participate in PIM. If this command is not present in the configuration then there are no restrictions.

Multicast routing and PIM must be enabled for this command to appear in the configuration. If you disable multicast routing, this command is removed from the configuration.

Examples

The following example allows the router with the IP address 10.1.1.1 to become a PIM neighbor on interface GigabitEthernet0/2:

```
hostname(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
hostname(config)# access-list pim_filter deny any
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim old-register-checksum

To allow backward compatibility on a rendezvous point (RP) that uses old register checksum methodology, use the **pim old-register-checksum** command in global configuration mode. To generate PIM RFC-compliant registers, use the **no** form of this command.

pim old-register-checksum

no pim old-register-checksum

Syntax Description

This command has no arguments or keywords.

Defaults

The security appliance generates PIM RFC-compliant registers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance software accepts register messages with checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS method—accepting register messages with the entire PIM message for all PIM message types. The **pim old-register-checksum** command generates registers compatible with Cisco IOS software.

Examples

The following example configures the security appliance to use the old checksum calculations:

```
hostname(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim rp-address

To configure the address of a PIM rendezvous point (RP), use the **pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

Syntax Description

acl	(Optional) The name or number of a standard access list that defines which multicast groups the RP should be used with. Do not use a host ACL with this command.
bidir	(Optional) Indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM sparse mode.
ip_address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

No PIM RP addresses are configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain require knowledge of the well-known PIM RP address. The address is statically configured using this command.

Note The security appliance does not support Auto-RP; you must use the **pim rp-address** command to specify the RP address.

You can configure a single RP to serve more than one group. The group range specified in the access list determines the PIM RP group mapping. If the an access list is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

Note The security appliance always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Examples

The following example sets the PIM RP address to 10.0.0.1 for all multicast groups:

```
hostname(config)# pim rp-address 10.0.0.1
```

Related Commands

Command	Description
pim accept-register	Configures candidate RPs to filter PIM register messages.

pim spt-threshold infinity

To change the behavior of the last hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

Syntax Description

group-list *acl*	(Optional) Indicates the source groups restricted by the access list. The *acl* argument must specify a standard ACL; extended ACLs are not supported.

Defaults

The last hop PIM router switches to the shortest-path source tree by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If the **group-list** keyword is not used, this command applies to all multicast groups.

Examples

The following example causes the last hop PIM router to always use the shared tree instead of switching to the shortest-path source tree:

```
hostname(config)# pim spt-threshold infinity
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

ping

To determine if other IP addresses are visible from the security appliance, use the **ping** command in privileged EXEC mode.

ping [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

Syntax Description

data *pattern*	(Optional) Specifies the 16-bit data pattern in hexidecimal.
host	Specifies the IPv4 or IPv6 address or name of the host to ping. The name can be a DNS name or a name assigned with the **name** command. The maximum number of characters for DNA names is 128, and the maximum number of characters for names created with the **name** command is 63.
if_name	(Optional) Specifies the interface name, as configured by the **nameif** command, by which the *host* is accessible. If not supplied, then the *host* is resolved to an IP address and then the routing table is consulted to determine the destination interface.
repeat *count*	(Optional) Specifies the number of times to repeat the ping request.
size *bytes*	(Optional) Specifies the datagram size in bytes.
timeout *seconds*	(Optional) Specifies the the number of seconds to wait before timing out the ping request.
validate	(Optional) Specifies to validate reply data.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	Support for DNS names added.

Usage Guidelines

The **ping** command allows you to determine if the security appliance has connectivity or if a host is available on the network. If the security appliance has connectivity, ensure that the **icmp permit any** *interface* command is configured. This configuration is required to allow the security appliance to respond and accept messages generated from the **ping** command. The **ping** command output shows if the response was received. If a host is not responding, when you enter the **ping** command, a message similar to the following displays:

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Use the **show interface** command to ensure that the security appliance is connected to the network and is passing traffic. The address of the specified *if_name* is used as the source address of the ping.

If you want internal hosts to ping external hosts, you must do one of the following:

- Create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list acl_grp permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.
- Configure the ICMP inspection engine using the **inspect icmp** command. For example, adding the **inspect icmp** command to the **class default_inspection** class for the global service policy allows echo replies through the security appliance for echo requests initiated by internal hosts.

You can also perform an extended ping, which allows you to enter the keywords one line at a time.

If you are pinging through the security appliance between hosts or routers, but the pings are not successful, use the **capture** command to monitor the success of the ping.

The security appliance **ping** command does not require an interface name. If you do not specify an interface name, the security appliance checks the routing table to find the address that you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

Examples

The following example shows how to determine if other IP addresses are visible from the security appliance:

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example specifies a host using a DNS name:

```
hostname# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following is an example of an extended ping:

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Related Commands

Command	Description
capture	Captures packets at an interface
icmp	Configures access rules for ICMP traffic that terminates at an interface.
show interface	Displays information about the VLAN configuration.

police

To apply QoS policing to a class map, use the **police** command in class configuration mode. To remove the rate-limiting requirement, use the **no** form of this command. Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the security appliance drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

no police

Syntax Description

conform-burst	Specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512000000 bytes.
conform-action	Sets the action to take when the rate is less than the *conform_burst* value.
conform-rate	Sets the rate limit for this traffic flow; between 8000 and 2000000000 bits per second.
drop	Drops the packet.
exceed-action	Sets the action to take when the rate is between the *conform-rate* value and the *conform-burst* value.
input	Enables policing of traffic flowing in the input direction.
output	Enables policing of traffic flowing in the output direction.
transmit	Transmits the packet.

Defaults

No default behavior or variables.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Added the **input** option. Policing traffic in the inbound direction is now supported.

Usage Guidelines

To enable policing, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform policing.

2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **police**—Enable policing for the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

Note The **police** command merely enforces the maximum speed and burst rate, forcing them to the conforming rate value. It does not enforce the **conform-action** or the **exceed-action** specification if these are present.

You can configure each of the QoS features alone if desired for the security appliance. Often, though, you configure multiple QoS features on the security appliance so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).

  You cannot configure priority queueing and policing for the same set of traffic.
- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the security appliance does not restrict you from configuring this.

If a service policy is applied or removed from an interface that has existing VPN client/LAN-to-LAN or non-tunneled traffic already established, the QoS policy is not applied or removed from the traffic stream. To apply or remove the QoS policy for such connections, you must clear (that is, drop) the connections and re-establish them.

Examples

The following is an example of a **police** command for the output direction that sets the conform rate to 100,000 bits per second, a burst value of 2,000,000 bytes, and specifies that traffic that exceeds the burst rate will be dropped:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class-map firstclass
hostname(config-cmap)# class localclass
hostname(config-pmap-c)# police output 100000 20000 exceed-action drop
hostname(config-cmap-c)# class class-default
hostname(config-pmap-c)#
```

The following example shows how to do rate-limiting on traffic destined to an internal web server.

```
hostname# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
hostname# class-map http_traffic
hostname(config-cmap)# match access-list http_traffic
hostname(config-cmap)# policy-map outside_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# police input 56000
hostname(config-pmap-c)# service-policy outside_policy interface outside
hostname(config)#
```

Related Commands

class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

policy

To specify the source for retrieving the CRL, use the **policy** command in ca-crl configuration mode.

policy {**static | cdp | both**}

Syntax Description

both	Specifies that if obtaining a CRL using the CRL distribution point fails, retry using static CDPs up to a limit of five.
cdp	Uses the CDP extension embedded within the certificate being checked. In this case, the security appliance retrieves up to five CRL distributions points from the CDP extension of the certificate being verified and augments their information with the configured default values, if necessary. If the security appliance attempt to retrieve a CRL using the primary CDP fails, it retries using the next available CDP in the list. This continues until either the security appliance retrieves a CRL or exhausts the list.
static	Uses up to five static CRL distribution points. If you specify this option, specify also the LDAP or HTTP URLs with the **protocol** command.

Defaults

The default setting is **cdp**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CRL configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and configures CRL retrieval to occur using the CRL distribution point extension in the certificate being checked or if that fails, to use static CDPs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
url	Creates and maintains a list of static URLs for retrieving CRLs.

policy-map

When using the Modular Policy Framework, assign actions to traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command) by using the **policy-map** command (without the **type** keyword) in global configuration mode. To remove a Layer 3/4 policy map, use the **no** form of this command.

policy-map *name*

no policy-map *name*

Syntax Description

name	Specifies the name for this policy map up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

The maximum number of policy maps is 64. You can identify multiple Layer 3/4 class maps in a Layer 3/4 policy map (see the **class** command), and you can assign multiple actions from one or more feature types to each class map.

A packet can match only one class map in the policy map for each feature type. When the packet matches a class map for a feature type, the security appliance does not attempt to match it to any subsequent class maps for that feature type. If the packet matches a subsequent class map for a different feature type, however, then the security appliance also applies the actions for the subsequent class map. For example,

if a packet matches a class map for connection limits, and also matches a class map for application inspection, then both class map actions are applied. If a packet matches a class map for application inspection, but also matches another class map for application inspection, then the second class map actions are not applied.

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions.

Note When you use a global policy, all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally. Because the policy is applied to all interfaces, the policy will be applied in both directions so bidirectionality in this case is redundant.

For features that are applied unidirectionally, for example QoS, only traffic that exits the interface to which you apply the policy map is affected. See Table 22-1 for the directionality of each feature.

Table 22-1 Feature Directionality

Feature	Single Interface Direction	Global Direction
TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
CSC	Bidirectional	Ingress
Application inspection	Bidirectional	Ingress
IPS	Bidirectional	Ingress
QoS policing	Egress	Egress
QoS priority queue	Egress	Egress

The order in which different types of actions in a policy map are performed is independent of the order in which the actions appear in the policy map. Actions are performed in the following order:

- TCP normalization, TCP and UDP connection limits and timeouts, and TCP sequence number randomization

Note When a the security appliance performs a proxy service (such as AAA or CSC) or it modifies the TCP payload (such as FTP inspection), the TCP normalizer acts in dual mode, where it is applied before and after the proxy or payload modifying service.

- CSC
- Application inspection
- IPS
- QoS policing
- QoS priority queue

You can only assign one policy map per interface, but you can apply the same policy map to multiple interfaces.

The configuration includes a default Layer 3/4 policy map that the security appliance uses in the default global policy. It is called **global_policy** and performs inspection on the default inspection traffic. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.

The default policy map configuration includes the following commands:

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

Examples

The following is an example of a **policy-map** command for connection policy. It limits the number of connections allowed to the web server 10.1.1.1:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
```

```
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the security appliance does not make this match because they previously matched other classes.

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
clear configure policy-map	Removes all policy map configuration. If a policy map is in use in a **service-policy** command, that policy map is not removed.
class-map	Defines a traffic class map.
service-policy	Assigns the policy map to an interface or globally to all interfaces.
show running-config policy-map	Display all current policy map configurations.

policy-map type inspect

When using the Modular Policy Framework, define special actions for inspection application traffic by using the **policy-map type inspect** command in global configuration mode. To remove an inspection policy map, use the **no** form of this command.

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

Syntax Description

application	Specifies the type of application traffic you want to act upon. Available types include: • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **sip** • **skinny** • **snmp**
policy_map_name	Specifies the name for this policy map up to 40 characters in length. Names that begin with "_internal" or "_default" are reserved and cannot be used. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

An inspection policy map consists of one or more of the following commands entered in policy-map configuration mode. The exact commands available for an inspection policy map depends on the application.

- **match** command—You can define a **match** command directly in the inspection policy map to match application traffic to criteria specific to the application, such as a URL string. Then you enable actions in match configuration mode such as **drop**, **reset**, **log**, and so on. The **match** commands available depend on the application.
- **class** command—This command identifies an inspection class map in the policy map (see the **class-map type inspect** command to create the inspection class map). An inspection class map includes **match** commands that match application traffic with criteria specific to the application, such as a URL string, for which you then enable actions in the policy map. The difference between creating a class map and using a **match** command directly in the inspection policy map is that you can group multiple matches, and you can reuse class maps.
- **parameters** command—Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

You can specify multiple **class** or **match** commands in the policy map.

Some **match** commands can specify regular expressions to match text inside a packet. See the **regex** command and the **class-map type regex** command, which groups multiple regular expressions.

The default inspection policy map configuration includes the following commands, which sets the maximum message length for DNS packets to be 512 bytes:

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

If a packet matches multiple different **match** or **class** commands, then the order in which the security appliance applies the actions is determined by internal security appliance rules, and not by the order they are added to the policy map. The internal rules are determined by the application type and the logical progression of parsing a packet, and are not user-configurable. For example for HTTP traffic, parsing a

Request Method field precedes parsing the Header Host Length field; an action for the Request Method field occurs before the action for the Header Host Length field. For example, the following match commands can be entered in any order, but the **match request method get** command is matched first.

```
hostname(config-pmap)# match request header host length gt 100
hostname(config-pmap-c)# reset
hostname(config-pmap-c)# match request method get
hostname(config-pmap-c)# log
```

If an action drops a packet, then no further actions are performed. For example, if the first action is to reset the connection, then it will never match any further **match** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. (You can configure both the **reset** (or **drop-connection**, and so on.) and the **log** action for the same **match** command, in which case the packet is logged before it is reset for a given match.)

If a packet matches multiple **match** or **class** commands that are the same, then they are matched in the order they appear in the policy map. For example, for a packet with the header length of 1001, it will match the first command below, and be logged, and then will match the second command and be reset. If you reverse the order of the two **match** commands, then the packet will be dropped and the connection reset before it can match the second **match** command; it will never be logged.

```
hostname(config-pmap)# match request header length gt 100
hostname(config-pmap-c)# log
hostname(config-pmap-c)# match request header length gt 1000
hostname(config-pmap-c)# reset
```

A class map is determined to be the same type as another class map or **match** command based on the lowest priority **match** command in the class map (the priority is based on the internal rules). If a class map has the same type of lowest priority **match** command as another class map, then the class maps are matched according to the order they are added to the policy map. If the lowest priority command for each class map is different, then the class map with the higher priority **match** command is matched first.

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy inbound_policy interface outside
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
parameters	Enters parameter configuration mode for an inspection policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

policy-server-secret

To configure a secret key used to encrypt authentication requests to a SiteMinder SSO server, use the **policy-server-secret** command in webvpn-sso-siteminder configuration mode. To remove a secret key, use the **no** form of this command.

policy-server-secret *secret-key*

no policy-server-secret

Note This command is required for SiteMinder SSO authentication.

Syntax Description

secret-key	The character string used as a secret key to encrypt authentication communications. There is no minimum or maximum number of characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Config-webvpn-sso-siteminder configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. You first create the SSO server using the **sso-server** command. For SiteMinder SSO servers, the **policy-server-secret** command secures authentication communications between the security appliance and the SSO server.

The command argument, *secret-key*, is similar to a password: you create it, save it, and configure it. It is configured on both the security appliance using the `policy-server-secret` command and on the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

This command applies only to the SiteMinder type of SSO server.

Examples

The following command, entered in config-webvpn-sso-siteminder mode and including a random character string as an argument, creates a secret key for SiteMinder SSO server authentication communications:

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
hostname(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

polltime interface

To specify the data interface poll and hold times in an Active/Active failover configuration, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface [**msec**] *time* [**holdtime** *time*]

no polltime interface [**msec**] *time* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a data interface must receive a hello message from the peer interface, after which the peer interface is declared failed. Valid values are from 5 to 75 seconds.
interface *time*	Specifies data interface polling period. Valid values are from 3 to 15 seconds. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Defaults

The poll *time* is 5 seconds.

The **holdtime** *time* is 5 times the poll *time*.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The command was changed to include the optional **holdtime** *time* value and the ability to specify the poll time in milliseconds.

Usage Guidelines

Use the **polltime interface** command to change the frequency that hello packets are sent out on interfaces associated with the specified failover group. This command is available for Active/Active failover only. Use the **failover polltime interface** command in Active/Standby failover configurations.

You cannot enter a **holdtime** value that is less than 5 times the poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested. Interface testing begins when a hello packet is not heard on the interface for over half the hold time.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following partial example shows a possible configuration for a failover group. The interface poll time is set to 500 milliseconds and the hold time to 5 seconds for data interfaces in failover group 1.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Specifies the unit failover poll and hold times.
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.

pop3s

To enter POP3S configuration mode, use the **pop3s** command in global configuration mode. To remove any commands entered in POP3S command mode, use the **no** version of this command.

POP3 is a client/server protocol in which your Internet server receives and holds e-mail for you. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. This standard protocol is built into most popular e-mail products. POP3S lets you receive e-mail over an SSL connection.

pop3s

no pop3

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to enter POP3S configuration mode:

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.
show running-config pop3s	Displays the running configuration for POP3S.

port

To specify the port an e-mail proxy listens to, use the **port** command in the applicable e-mail proxy command mode. To revert to the default value, use the **no** version of this command.

port {*portnum*}

no port

Syntax Description

portnum	The port for the e-mail proxy to use. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Defaults

The default ports for e-mail proxies are as follows:

E-mail Proxy	Default Port
IMAP4S	993
POP3S	995
SMTPS	988

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Examples

The following example shows how to set port 1066 for the IMAP4S e-mail proxy:

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

port-forward

To configure the set of applications that users of clientless SSL VPN session can access over forwarded TCP ports, use the **port-forward** command in webvpn configuration mode.

port-forward {*list_name local_port remote_server remote_port description*}

To configure access to multiple applications, use this command with the same *list_name* multiple times, once for each application.

To remove a configured application from a list, use the **no port-forward** *list_name local_port* command (you need not include the *remote_server* and *remote_port* parameters).

no port-forward *listname localport*

To remove an entire configured list, use the **no port-forward** *list_name* command.

no port-forward *list_name*

Syntax Description

description	Provides the application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.
list_name	Groups the set of applications (forwarded TCP ports) users of clientless SSL VPN sessions can access. Maximum 64 characters.
local_port	Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *list_name*. Enter a port number in the range 1-65535. To avoid conflicts with existing services, use a port number greater than 1024.
remote_port	Specifies the port to connect to for this application on the remote server. This is the actual port the application uses. Enter a port number in the range 1-65535 or port name.
remote_server	Provides the DNS name or IP address of the remote server for an application. We recommend using a DNS name. If you enter the IP address, you may enter it in either IPv4 or IPv6 format.

Defaults

There is no default port forwarding list.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.
8.0(2)	The command mode was changed to webvpn.

Usage Guidelines

The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. Neither port forwarding nor the smart tunnel feature that provides application access through a clientless SSL VPN session supports MAPI. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.

Examples

The following table shows the values used for example applications.

Application	Local Port	Server DNS Name	Remote Port	Description
IMAP4S e-mail	20143	IMAP4Sserver	143	Get Mail
SMTPS e-mail	20025	SMTPSserver	25	Send Mail
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

The following example shows how to create a port forwarding list called *SalesGroupPorts* that provides access to these applications:

```
hostname(config)# webvpn
hostname(config-webvpn)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

Related Commands

Command	Description
port-forward auto-start	Entered in group-policy webvpn or username webvpn mode, this command starts port forwarding automatically and assigns the specified port forwarding list when the user logs onto a clientless SSL VPN session.
port-forward enable	Entered in group-policy webvpn or username webvpn mode, this command starts assigns the specified port forwarding list when the user logs on, but requires the user to start port forwarding manually, using the **Application Access** > **Start Applications** button on the clientless SSL VPN portal page.
port-forward disable	Entered in group-policy webvpn or username webvpn mode, this command turns off port forwarding.

port-forward-name

To configure the display name that identifies TCP port forwarding to end users for a particular user or group policy, use the **port-forward-name** command in webvpn mode, which you enter from group-policy or username mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** use the no form of the command. The **no** option restores the default name, "Application Access." To prevent a display name, use the **port-forward none** command.

port-forward-name {**value** *name* | **none**}

no port-forward-name

Syntax Description

none	Indicates that there is no display name. Sets a null value, thereby disallowing a display name. Prevents inheriting a value.
value *name*	Describes port forwarding to end users. Maximum of 255 characters.

Defaults

The default name is "Application Access."

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set the name, "Remote Access TCP Applications," for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

port-object

To add a port object to a service object group, use the **port-object** command in service configuration mode. To remove port objects, use the **no** form of this command.

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

Syntax Description

begin_service	Specifies the decimal number or name of a TCP or UDP port that is the beginning value for a range of services. This value must be between 0 and 65535.
end_service	Specifies the decimal number or name of a TCP or UDP port that is the ending value for a range of services. ervices. This value must be between 0 and 65535.
eq service	Specifies the decimal number or name of a TCP or UDP port for a service object.
range	Specifies a range of ports (inclusive).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Service configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **port-object** command is used with the **object-group** command to define an object that is either a specific service (port) or a range of services (ports) in service configuration mode.

If a name is specified for a TCP or UDP service, it must be one of the supported TCP or/and UDP names, and must be consistent with the protocol type of the object group. For instance, for a protocol types of tcp, udp, and tcp-udp, the names must be a valid TCP service name, a valid UDP service name, or a valid TCP and UDP service name, respectively.

If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object.

The following service names are supported:

TCP	UDP	TCP and UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

This example shows how to use the **port-object** command in service configuration mode to create a new port (service) object group:

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
hostname(config-service)# port-object eq snmp
```

```
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

post-max-size

To specify the maximum size allowed for an object to post, use the **post-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

post-max-size <*size*>

no post-max-size

Syntax Description

size	Specifies the maximum size allowed for a posted object. The range is 0 through 2147483647.

Defaults

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Setting the size to 0 effectively disallows object posting.

Examples

The following example sets the maximum size for a posted object to 1500 bytes:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# post-max-size 1500
```

Related Commands

Command	Description
download-max-size	Specifies the maximum size of an object to download.
upload-max-size	Specifies the maximum size of an object to upload.

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

pppoe client route distance

To configure an administrative distance for routes learned through PPPoE, use the **pppoe client route distance** command in interface configuration mode. To restore teh default setting, use the **no** form of this command.

pppoe client route distance *distance*

no pppoe client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through PPPoE. Valid values are from 1 to 255.

Defaults

Routes learned through PPPoE are given an administrative distance of 1 by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client route distance** command is checked only when a route is learned from PPPoE. If the **pppoe client route distance** command is entered after a route is learned from PPPoE, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enablgin PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client route track

To configure the PPPoE client to associate added routes with a specified tracked object number, use the **pppoe client route track** command in interface configuration mode. To remove the PPPoE route tracking, use the **no** form of this command.

pppoe client route track *number*

no pppoe client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client route track** command is checked only when a route is learned from PPPoE. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
```

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client secondary

To configure the PPPoE client to register as a client of a tracked object and to be brought up or down based on the tracking state, use the **pppoe client secondary** command in interface configuration mode. To remove the client registration, use the **no** form of this command.

pppoe client secondary track *number*

no pppoe client secondary track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client secondary** command is checked only when PPPoE session starts. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
```

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.

pre-fill-username

To enable extracting a username from a client certificate for use in authentication and authorization, use the **pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

pre-fill-username {**ssl-client** | **clientless**}

no pre-fill-username

Syntax Description

ssl-client	Enables this feature for AnyConnect VPN client connections.
clientless	Enables this feature for clientless connections.

Defaults

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **username-from-certificate** command as the username for username/password authentication and authorization. To use this pre-fill username from certificate feature, you must configure both commands.

To enable this feature, you must also configure the **usesrname-from-certificate** command in tunnel-group general-attributes mode.

Note In Release 8.0.4, the username is not pre-filled; instead, any data sent in the username field is ignored.

Examples

The following example, entered in global configuration mode, creates an IPSec remote access tunnel group named remotegrp and specifies that the name for an authentication or authorization query for an SSL VPN client must be derived from a digital certificate:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp webvpn-attributes
```

```
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

preempt

To cause the unit to become active on boot if it has the higher priority, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]

no preempt [*delay*]

Syntax Description

seconds	The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Defaults

By default, there is no delay.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). However, if one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Note If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
hostname(config)# failover group 1
```

```
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

To create an entry in a prefix list for ABR type 3 LSA filtering, use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network*/*len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network*/*len* [**ge** *min_value*] [**le** *max_value*]

Syntax Description

/	A required separator between the *network* and *len* values.
deny	Denies access for a matching condition.
ge *min_value*	(Optional) Specifies the minimum prefix length to be matched. The value of the *min_value* argument must be greater than the value of the *len* argument and less than or equal to the *max_value* argument, if present.
le *max_value*	(Optional) Specifies the maximum prefix length to be matched. The value of the *max_value* argument must be greater than or equal to the value of the *min_value* argument, if present, or greater than the value of the *len* argument if the *min_value* argument is not present.
len	The length of the network mask. Valid values are from 0 to 32.
network	The network address.
permit	Permits access for a matching condition.
prefix-list-name	The name of the prefix list. The prefix-list name cannot contain spaces.
seq *seq_num*	(Optional) Applies the specified sequence number to the prefix list being created.

Defaults

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The security appliance begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a mach is made, the security appliance does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network*/*len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified.The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

len < *min_value* <= *max_value* <= 32

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix10.0.0.0/8:

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

prefix-list-name	The name of a prefix list.
text	The text of the prefix list description. You can enter a maximum of 80 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
```

!

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Defaults

Prefix list sequence numbering is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Only the **no** form of this command appears in the configuration. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples

The following example disables prefix list sequence numbering:

```
hostname(config)# no prefix-list sequence-number
```

Related Commands

Command	Description
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

pre-shared-key

To specify a preshared key to support IKE connections based on preshared keys, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

pre-shared-key *key*

no pre-shared-key

Syntax Description

key	Specifies an alphanumeric key between 1 and 128 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPSec tunnel-group types.

Examples

The following command entered in config-ipsec configuration mode, specifies the preshared key XYZX to support IKE connections for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

primary

To give the primary unit higher priority for a failover group, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary

no primary

Syntax Description

This command has no arguments or keywords.

Defaults

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). If one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
```

```
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
secondary	Gives the secondary unit a higher priority than the primary unit.

priority

To enable QoS priority queueing, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queueing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or variables.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface (see the **priority-queue** command), while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue (the **shape** command). A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queueing:
  - Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.

- Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
- For IPSec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
- IPSec-over-TCP is not supported for priority traffic classification.

Configuring QoS with Modular Policy Framework

To enable priority queueing, use the Modular Policy Framework. You can use standard priority queueing or hierarchical priority queueing.

For standard priority queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

For hierarchical priority-queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.
   c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following is an example of the **priority** command in policy-map mode:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

Related Commands

class	Specifies a class map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.

policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

priority (vpn load balancing)

To set the priority of the local device participating in the virtual load-balancing cluster, use the **priority** command in VPN load-balancing mode. To revert to the default priority specification, use the **no** form of this command.

priority *priority*

no priority

Syntax Description

priority	The priority, in the range of 1 to 10, that you want to assign to this device.

Defaults

The default priority depends on the model number of the device:

Model Number	Default Priority
5520	5
5540	7

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
VPN load-balancing	—	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

This command sets the priority of the local device participating in the virtual load-balancing cluster.

The priority must be an integer in the range of 1 (lowest) to 10 (highest).

The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster. See *Cisco ASA 5500 Series Configuration Guide using the CLI* for details about the master-election process.

The **no** form of the command reverts the priority specification to the default value.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **priority** command that sets the priority of the current device to 9:

```
hostname(config)# interface GigabitEthernet 0/1
```

```
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

priority-queue *interface-name*

no priority queue *interface-name*

Syntax Description

interface-name	Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505, the name of the VLAN interface.

Defaults

By default, priority queuing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface that yopu create using the **priority-queue** command, while all other traffic goes into the “best effort” queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size (the **queue-limit** command). You can also fine-tune the maximum number of packets allowed into the transmit queue (the **tx-ring-limit** command). These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue-limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

Related Commands

Command	Description
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure priority-queue	Removes the current priority queue configuration.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.

privilege

To configure command privilege levels for use with command authorization (local, RADIUS, and LDAP (mapped) only), use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

no privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege only for the clear form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
command *command*	Specifies the command you are configuring. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately. Also, you cannot configure the privilege level of subcommands separately from the main command. For example, you can configure the **context** command, but not the **allocate-interface** command, which inherits the settings from the **context** command.
configure	(Optional) Sets the privilege only for the configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
level *level*	Specifies the privilege level; valid values are from 0 to 15. Lower privilege level numbers are lower privilege levels.
mode enable	(Optional) If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The **mode enable** keyword specifies both user EXEC mode and privileged EXEC mode.
mode configure	(Optional) If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The mode **configure** keyword specifies configuration mode, accessed using the **configure terminal** command.
show	(Optional) Sets the privilege only for the show form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.

Defaults

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**

- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

To view all privilege levels, see the **show running-config all privilege all** command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	Support for RADIUS users with Cisco VSA CVPN3000-Privilege-Level was added. LDAP users are supported if you map the LDAP attribute to the CVPN3000-Privilege-Level using the **ldap map-attributes** command.

Usage Guidelines

The **privilege** command lets you set privilege levels for security appliance commands when you configure the **aaa authorization command LOCAL** command. Even though the command uses the **LOCAL** keyword, this keyword enables local, RADIUS, and LDAP (mapped) authorization.

Examples

For example, the **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. For example, set each form separately as follows.

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

Alternatively, you can set all filter commands to the same level:

```
hostname(config)# privilege level 5 command filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level.

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

This example shows an additional command, the **configure** command, that uses the **mode** keyword:

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

Note This last line is for the **configure terminal** command.

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show curpriv	Display current privilege level.
show running-config privilege	Display privilege levels for commands.

prompt

To customize the CLI prompt, use the **prompt** command in global configuration mode. To revert to the default prompt, use the **no** form of this command.

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]}

no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]

Syntax Description

context	(Multiple mode only) Displays the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
priority	Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the **failover lan unit** command.
state	Displays the traffic-passing state of the unit. The following values are displayed for the state keyword: • act—Failover is enabled, and the unit is actively passing traffic. • stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. • actNoFailover—Failover is not enabled, and the unit is actively passing traffic. • stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit.

Defaults

The default prompt is the hostname. In multiple context mode, the hostname is followed by the current context name (*hostname*/*context*).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/).

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

The ability to add information to a prompt allows you to see at-a-glance which security appliance you are logged into when you have multiple modules. During a failover, this feature is useful when both security appliances have the same hostname.

Examples

The following example shows all available elements in the prompt:

```
hostname(config)# prompt hostname context priority state
```

The prompt changes to the following string:

```
hostname/admin/pri/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

protocol-enforcement

To enable the domain name, label length, and format check, including compression and looped pointer check, use the **protocol-enforcement** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

protocol-enforcement

no protocol-enforcement

Syntax Description

This command has no arguments or keywords.

Defaults

Protocol enforcement is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no protocol-enforcement** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Under certain conditions, protocol enforcement is performed even if the command is disabled. This occurs when parsing a DNS resource record is required for other purposes, such as DNS resource record classification, NAT or TSIG check.

Examples

The following example shows how to enable protocol enforcement in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP). To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

protocol http

no protocol http

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit HTTP.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca-CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If you use this command, be sure to assign HTTP rules to the public interface filter.

Examples

The following example enters ca-crl configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol ldap

no protocol ldap

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit LDAP.

Command Modes

The following table shows the modes in which you can enter thecommand:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in crl configure mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol scep

no protocol scep

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit SCEP.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol ldap	Specifies LDAP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the **protocol-object** command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*

no protocol-object *protocol*

Syntax Description

protocol	Protocol name or number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Protocol configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

protocol-violation

To define actions when a protocol violation occurs with HTTP and NetBIOS inspection, use the **protocol-violation** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

protocol-violation action [**drop** [**log**] | **log**]

no protocol-violation action [**drop** [**log**] | **log**]

Syntax Description

drop	Specifies to drop packets that do not conform to the protocol.
log	Specifies to log the protocol violations.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an HTTP or NetBIOS policy map. A syslog is issued when the HTTP or NetBIOS parser cannot detect a valid HTTP or NetBIOS message in the first few bytes of the message. This occurs, for instance, when a chunked encoding is malformed and the message cannot be parsed.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation action drop
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

proxy-bypass

To configure the security appliance to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML—use the **proxy-bypass** command in webvpn configuration mode. To disable proxy bypass, use the **no** form of the command.

proxy-bypass interface *interface name* **{port** *port number*| **path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* **{port** *port number*| **path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

Syntax Descriptionl

host	Identifies the host to forward traffic to. Use either the host IP address or a hostname.
interface	Identifies the ASA interface for proxy bypass.
interface name	Specifies an ASA interface by name.
link	Specifies rewriting of absolute external links.
none	Specifies no rewriting.
path-mask	Specifies the pattern to match.
path-mask	Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 128 bytes.
port	Identifies the port reserved for proxy bypass.
port number	Specifies a high numbered port reserved for proxy bypass. The port range is 20000-21000. You can use a port for one proxy bypass rule only.
rewrite	(Optional) Specifies the additional rules for rewriting: none or a combination of XML and links.
target	Identifies the remote server to forward the traffic to.
url	Enter the URL in the format **http(s)://***fully_qualified_domain_name*[:*port*]. Maximum 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
xml	Specifies rewriting XML content.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
WebVPN configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use proxy bypass for applications and web resources that work better with minimum content rewriting. The proxy-bypass command determines how to treat specific web applications that travel through the security appliance.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the security appliance. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.mycompany.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.mycompany.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

Examples

The following example shows how to configure the security appliance to use port 20001 for proxy bypass over the webvpn interface, using HTTP and its default port 80, to forward traffic to mycompany.site.com and to rewrite XML content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://mycompany.site.com rewrite xml
```

The next example shows how to configure the security appliance to use the path mask mypath/* for proxy bypass on the outside interface, using HTTP and its default port 443 to forward traffic to mycompany.site.com, and to rewrite XML and link content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://mycompany.site.com rewrite xml,link
```

Related Commands-

Command	Description
apcf	Specifies nonstandard rules to use for a particular application
rewrite	Determines whether traffic travels through the security appliance.

proxy-ldc-issuer

To issue TLS proxy local dynamic certificates, use the **proxy-ldc-issuer** command in crypto ca trustpoint configuration mode. To remove the configuration, use the **no** form of this command.

proxy-ldc-issuer

no proxy-ldc-issuer

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **proxy-ldc-issuer** command to issue TLS proxy local dynamic certificates. The **proxy-ldc-issuer** command grants a crypto trustpoint the role as local CA to issue the LDC and can be accessed from crypto ca trustpoint configuration mode.

The **proxy-ldc-issuer** command defines the local CA role for the trustpoint to issue dynamic certificates for TLS proxy. This command can only be configured under a trustpoint with “enrollment self.”

Examples

The following example shows how to create an internal local CA to sign the LDC for phones. This local CA is created as a regular self-signed trustpoint with **proxy-ldc-issuer** enabled.

```
hostname(config)# crypto ca trustpoint ldc_server
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# proxy-ldc-issuer
hostname(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
hostname(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
hostname(config-ca-trustpoint)# keypair ldc_signer_key
hostname(config)# crypto ca enroll ldc_server
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

proxy-server

To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, use the **proxy-server** command in phone-proxy configuration mode. To remove the HTTP proxy configuration from the Phone Proxy, use the **no** form of this command.

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

Syntax Description

interface *ifc*	Specifies the interface on which the HTTP proxy resides on the security appliance.
ip_address	Specifies the IP address of the HTTP proxy.
listen_port	Specifies the listening port of the HTTP proxy. If not specified, the default will be 8080.

Defaults

If the listen port is not specified, the port is configured to be 8080 by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.

The *ip_address* you enter should be the global IP address based on where the IP phone and HTTP proxy server is located.

If the proxy server is located in a DMZ and the IP phones are located outside the network, the security appliance does a lookup to see if there is a NAT rule and uses the global IP address to write into the configuration file.

You can enter a hostname in the *ip_address* argument when that hostname can be resolved to an IP address by the security appliance (for example, DNS lookup is configured) because the security appliance will resolve the hostname to an IP address.

By default, the Phone URL Parameters configured under the Enterprise Parameters use an FQDN in the URLs. The parameters might need to be changed to use an IP address if the DNS lookup for the HTTP proxy does not resolve the FQDNs.

To make sure the proxy server URL was written correctly to the IP phones configuration files, check the URL on an IP phone under Settings > Device Configuration > HTTP configuration >Proxy Server URL.

The Phone Proxy does not inspect this HTTP traffic to the proxy server.

If the security appliance is in the path of the IP phone and the HTTP proxy server, use existing debugging techniques (such as syslogs and captures) to troubleshoot the proxy server.

You can configure only one proxy server while the Phone Proxy is in use; however, if the IP phones have already downloaded their configuration files after you have configured the proxy server, you must restart the IP phones so that they get the configuration file with the proxy server's address in the file.

Examples

The following example shows the use of the **proxy-server** command to configure the HTTP proxy server for the Phone Proxy:

```
hostname(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

publish-crl

To allow other security appliances to validate the revocation status of certificates issued by the Local CA, use the **publish-crl** command in config-ca-server configuration mode to allow downloading of the CRL directly from and interface on the security appliance. To make the CRL unavailable for downloading, use the **no** form of this command.

[no] publish-crl interface *interface* **[port** *portnumber* **]**

Syntax Description

interface *interface*	Specifies the *nameif* used for the interface, such as **gigabitethernet0/1**. See the **interface** command for details.
port *portnumber*	Optional. Specifies the port on which the interface device expects to download the CRL. Port numbers can be in the range 1-65535.

Defaults

The default **publish-crl** status is **no publish**. TCP port 80 is the default for HTTP.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-ca-server	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The CRL is inaccessible by default. You must enable access to the CRL file on the interface and port required.

TCP port 80 is the HTTP default port number. If you configure a non-default port (other than port 80), be sure the **cdp-url** configuration includes the new port number so other devices know to access this specific port.

The CRL Distribution Point (CDP) is the location of the CRL on the Local CA security appliance. The URL you configure with the cdp-url command is embedded into any issued certificates. If you do not configure a specific location for the CDP, the default CDP url is: http://hostname.domain/+CSCOCA+/asa_ca.crl.

An HTTP redirect and a CRL download request are handled by the same HTTP listener, if Clientless SSL VPN is enabled on the same interface. The listener checks for the incoming URL and if it matches the one configured with the cdp-url command, the CRL file downloads. If the URL does not match the cdp-url, the connection is redirected to HTTPS (if 'http redirect' is enabled).

Examples

This publish-crl command example, entered in config-ca-server mode, enables port 70 of the outside interface for CRL download:

This **publish-crl** command example, entered in config-ca-server mode, enables port 70 for the outside for CRL download:

```
hostname(config)# crypto ca server
hostname (config-ca-server)#publish-crl outside 70
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies a particular location for the automatically generated CRL.
show interface	Displays the runtime status and statistics of interfaces.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

The root directory (/) is the default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is similar in functionality to the **dir** command.

Examples

The following example shows how to display the current working directory:

```
hostname# pwd
disk0:/
hostname# pwd
flash:
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
more	Displays the contents of a file.

CHAPTER 23

queue-limit through rtp-conformance Commands

queue-limit (priority-queue)

To specify the depth of the priority queues, use the **queue-limit** command in priority-queue mode. To remove this specification, use the **no** form of this command.

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets that can be queued (that is, buffered) before the interface begins dropping packets. See the Usage Notes section for the range of possible values.

Defaults

The default queue limit is 1024 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Priority-queue	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The security appliance recognizes priority traffic and enforces appropriate Quality of Service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.

You must use the **priority-queue** command to create the priority queue for an interface before priority queuing takes effect. You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue mode, as shown by the prompt. In priority-queue mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best -effort) allowed to be buffered before dropping packets (**queue-limit** command).

Note You *must* configure the **priority-queue** command in order to enable priority queueing for the interface.

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop*. To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Note The upper limit of the range of values for the **queue-limit** and **tx-ring-limit** commands is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device. The queues must not exceed the available memory. The theoretical maximum number of packets is 2147483647.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue-limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.

queue-limit (tcp-map)

To configure the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, use the **queue-limit** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

queue-limit *pkt_num* [**timeout** *seconds*]

no queue-limit

Syntax Description

pkt_num	Specifies the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, between 1 and 250. The default is 0, which means this setting is disabled and the default system queue limit is used depending on the type of traffic. See the "Usage Guidelines" section for more information.
timeout *seconds*	(Optional) Sets the maximum amount of time that out-of-order packets can remain in the buffer, between 1 and 20 seconds. The default is 4 seconds. If packets are not put in order and passed on within the timeout period, then they are dropped. You cannot change the timeout for any traffic if the *pkt_num* argument is set to 0; you need to set the limit to be 1 or above for the **timeout** keyword to take effect.

Defaults

The default setting is 0, which means this command is disabled.

The default timeout is 4 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)/8.0(4)	The **timeout** keyword was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **queue-limit**—In tcp-map configuration mode, you can enter the **queue-limit** command and many others.

2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

If you do not enable TCP normalization, or if the **queue-limit** command is set to the default of 0, which means it is disabled, then the default system queue limit is used depending on the type of traffic:

- Connections for application inspection (the **inspect** command), IPS (the **ips** command), and TCP check-retransmission (the TCP map **check-retransmission** command) have a queue limit of 3 packets. If the security appliance receives a TCP packet with a different window size, then the queue limit is dynamically changed to match the advertized setting.
- For other TCP connections, out-of-order packets are passed through untouched.

If you set the **queue-limit** command to be 1 or above, then the number of out-of-order packets allowed for all TCP traffic matches this setting. For application inspection, IPS, and TCP check-retransmission traffic, any advertized settings are ignored. For other TCP traffic, out-of-order packets are now buffered and put in order instead of passed through untouched.

Examples

The following example sets the queue limit to 8 packets and the buffer timeout to 6 seconds for all Telnet connections:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8 timeout 6
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

quit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **quit** command.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **quit** command in privileged or user EXEC modes, you log out from the security appliance. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **quit** command to exit global configuration mode, and then logout from the session:

```
hostname(config)# quit
hostname# quit

Logoff
```

The following example shows how to use the **quit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
hostname(config)# quit
hostname# disable
hostname>
```

Related Commands

Command	Description
exit	Exits a configuration mode or logs out from privileged or user EXEC modes.

radius-common-pw

To specify a common password to be used for all users who are accessing this RADIUS authorization server through this security appliance, use the **radius-common-pw** command in AAA-server host mode. To remove this specification, use the **no** form of this command:

radius-common-pw *string*

no radius-common-pw

Syntax Description

string	A case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with this RADIUS server.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
AAA-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Introduced in this release.

Usage Guidelines

This command is valid only for RADIUS authorization servers.

The RADIUS authorization server requires a password and username for each connecting user. The security appliance provides the username automatically. You enter the password here. The RADIUS server administrator must configure the RADIUS server to associate this password with each user authorizing to the server via this security appliance. Be sure to provide this information to your RADIUS server administrator.

If you do not specify a common user password, each user's password is his or her own username. For example, a user with the username "jsmith" would enter "jsmith". If you are using usernames for the common user passwords, as a security precaution do not use this RADIUS server for authorization anywhere else on your network.

Note This field is essentially a space-filler. The RADIUS server expects and requires it, but does not use it. Users do not need to know it.

Examples

The following example configures a RADIUS AAA server group named “svrgrp1” on host “1.2.3.4”, sets the timeout interval to 9 seconds, sets the retry interval to 7 seconds, and configures the RADIUS commnon password as “allauthpw”.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

radius-reject-message

To enable the display of a RADIUS reject message on the login screen when authentication is rejected, use the **radius-eject-message** command from tunnel-group webvpn attributes configuration mode. To remove the command from the configuration, use the **no** form of the command:

radius-reject-message

no radius-reject-message

Defaults

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Enable this command if you want to display to remote users a RADIUS message about an authentication failure.

Examples

The following example enables the display of a RADIUS rejection message for the connection profile named engineering:

```
hostname(config)# tunnel-group engineering webvpn-attributes
hostname(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (removed)

To have the security appliance use MS-CHAPv2 to negotiate a password update with the user during authentication, use the **radius-with-expiry** command in tunnel-group ipsec-attributes configuration mode. The security appliance ignores this command if RADIUS authentication has not been configured. To return to the default value, use the **no** form of this command.

radius-with-expiry

no radius-with-expiry

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated. The **password-management** command replaces it. The **no** form of the **radius-with-expiry** command is no longer supported.
8.0(2)	This command was deprecated.

Usage Guidelines

You can apply this attribute only to IPSec remote-access tunnel-group type.

Examples

The following example entered in config-ipsec configuration mode, configures Radius with Expiry for the remote-access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# radius-with-expiry
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
password-management	Enables password management. This command, in the tunnel-group general-attributes configuration mode, replaces the **radius-with-expiry** command.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

rate-limit

When using the Modular Policy Framework, limit the rate of messages for packets that match a **match** command or class map by using the **rate-limit** command in match or class configuration mode. This rate limit action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the **no** form of this command.

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

Syntax Description

messages_per_second	Limits the messages per second.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **rate-limit** command to limit the rate of messages.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

Examples

The following example limits the invite requests to 100 messages per second:

```
hostname(config-cmap)# policy-map type inspect sip sip-map1
hostname(config-pmap-c)# match request-method invite
hostname(config-pmap-c)# rate-limit 100
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

reactivation-mode

To specify the method by which failed servers in a group are reactivated, use the **reactivation-mode** command in aaa-server protocol mode. To remove this specification, use the **no** form of this command:

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

Syntax Description

deadtime *minutes*	(Optional) Specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent re-enabling of all servers. The default is 10 minutes.
depletion	Reactivates failed servers only after all of the servers in the group are inactive.
timed	Reactivates failed servers after 30 seconds of down time.

Defaults

The default reactivation mode is depletion, and the default deadtime value is 10.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server protcocol configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Each server group has an attribute that specifies the reactivation policy for its servers.

In **depletion** mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers. When **depletion** mode is in use, you can also specify the **deadtime** parameter. The **deadtime** parameter specifies the amount of time (in minutes) that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. This parameter is meaningful only when the server group is being used in conjunction with the local fallback feature.

In **timed** mode, failed servers are reactivated after 30 seconds of down time. This is useful when customers use the first server in a server list as the primary server and prefer that it is online whenever possible. This policy breaks down in the case of UDP servers. Since a connection to a UDP server will

not fail, even if the server is not present, UDP servers are put back on line blindly. This could lead to slowed connection times or connection failures if a server list contains multiple servers that are not reachable.

Accounting server groups that have simultaneous accounting enabled are forced to use the **timed** mode. This implies that all servers in a given list are equivalent.

Examples

The following example configures aTACACS+ AAA server named “srvgrp1” to use the depletion reactivation mode, with a deadtime of 15 minutes:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

The following example configures aTACACS+ AAA server named “srvgrp1” to use timed reactivation mode:

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)#
```

Related Commands

accounting-mode	Indicates whether accounting messages are sent to a single server or sent to all servers in the group.
aaa-server protocol	Enters AAA server group configuration mode so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

record-entry

To specify the trustpoints to be used for the creation of the CTL file, use the record-entry command in ctl-file configuration mode. To remove a record entry from a CTL, use the **no** form of this command.

record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

no record-entry [**capf** | **cucm** | **cucm-tftp** | **tftp**] **trustpoint** *trust_point* **address** *ip_address* [**domain-name** *domain_name*]

Syntax Description

capf	Specifies the role of this trustpoint to be CAPF. Only one CAPF trustpoint can be configured.
cucm	Specifies the role of this trustpoint to be CCM. Multiple CCM trustpoints can be configured.
cucm-tftp	Specifies the role of this trustpoint to be CCM+TFTP. Multiple CCM+TFTP trustpoints can be configured.
domain-name *domain_name*	(Optional) Specifies the domain name of the trustpoint used to create the DNS field for the trustpoint. This is appended to the Common Name field of the Subject DN to create the DNS Name. The domain name should be configured when the FQDN is not configured for the trustpoint.
address *ip_address*	Specifies the IP address of the trustpoint.
tftp	Specifies the role of this trustpoint to be TFTP. Multiple TFTP trustpoints can be configured.
trustpoint *trust_point*	Sets the name of the trustpoint installed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Only one domain-name can be specified. If the CTL file does not exist, manually export this certificate from CUCM to the security appliance.

Use this command only when you have not configured a CTL file for the Phone Proxy. Do not use this command when you have already configured a CTL file.

The IP address you specify in the *ip_address* argument must be the global address or address as seen by the IP phones because it will be the IP address used for the CTL record for the trustpoint.

Add additional record-entry configurations for each entity that is required in the CTL file.

Examples

The following example shows the use of the **record-entry** command to specify the trustpoints to be used for the creation of the CTL file:

```
hostname(config-ctl-file)# record-entry cucm-tftp trustpoint cucm1 address 192.168.1.2
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

redirect-fqdn

To enable or disable redirection using a fully-qualified domain name in vpn load-balancing mode, use the **redirect-fqdn enable** command in global configuration mode.

redirect-fqdn {enable | disable}

no redirect-fqdn {enable | disable}

Note To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

disable	Disables redirection with fully-qualified domain names.
enable	Enables redirection with fully-qualified domain names.

Defaults

This behavior is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a secondary device.

As a VPN cluster master, this security appliance can send a fully qualified domain name (FQDN), using reverse DNS lookup, of a cluster device (another security appliance in the cluster), instead of its outside IP address, when redirecting VPN client connections to that cluster device.

All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

To do WebVPN load Balancing using FQDNs rather than IP addresses, you must do the following configuration steps:

Step 1 Enable the use of FQDNs for Load Balancing with the **redirect-fqdn enable** command.

Step 2 Add an entry for each of your ASA outside interfaces into your DNS server, if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup.

Step 3 Enable DNS lookups on your ASA with the command - "dns domain-lookup inside" (or whichever interface has a route to your DNS server).

Step 4 Define your DNS server IP address on the ASA; for example: `dns name-server 10.2.3.4` (IP address of your DNS server)

Examples

The following is an example of the **redirect-fqdn** command that disables redirection:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# redirect-fqdn disable
hostname(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that enables redirection for a fully-qualified domain name, specifies the public interface of the cluster as "test" and the private interface of the cluster as "foo":

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# redirect-fqdn enable
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

redistribute (EIGRP)

To redistribute routes from one routing domain into the EIGRP routing process, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*]

Syntax Description

bandwidth	EIGRP bandwidth metric in Kilobits per second. Valid values are from 1 to 4294967295.
connected	Specifies redistributing a network connected to an interface into the EIGRP routing process.
delay	EIGRP delay metric, in 10 microsecond units. Valid values are from 0 to 4294967295.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
load	EIGRP effective bandwidth (loading) metric. Valid values are from 1 to 255, where 255 indicates 100% loaded.
match	(Optional) Specifies the conditions for redistributing routes from OSPF into EIGRP.
metric	(Optional) Specifies the values for the EIGRP metrics of routes redistributed into the EIGRP routing process.
mtu	The MTU of the path. Valid values are from 1 to 65535.
nssa-external *type*	Specifies the OSPF metric type for routes that are external to an NSSA; valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the EIGRP routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
reliability	EIGRP reliability metric. Valid values are from 0 to 255, where 255 indicates 100% reliability.
rip	Specifies redistributing a network from the RIP routing process into the EIGRP routing process.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the EIGRP routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into the EIGRP routing process.

Defaults

The following are the command defaults:

- **match**: **Internal**, **external 1**, **external 2**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You must specify the **metric** with the redistribute command if you do not have a **default-metric** command in your EIGRP configuration.

Examples

This example redistributes static and connected routes into the EIGRP routing process:

```
hostname(config)# router eigrp 100
hostname(config-router)# redistribute static
hostname(config-router)# redistribute connected
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redistribute (OSPF)

To redistribute routes from one routing domain into an OSPF routing process, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected** | **eigrp** *as-number*} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **rip** | **static** | **connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

Syntax Description

connected	Specifies redistributing a network connected to an interface into an OSPF routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the OSPF routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type *metric_type*	(Optional) The external link type associated with the default route advertised into the OSPF routing domain. It can be either of the following two values: **1** (Type 1 external route) or **2** (Type 2 external route).
nssa-external *type*	Specifies the OSPF metric type for routes that are external to an NSSA; valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the current OSPF routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
rip	Specifies redistributing a network from the RIP routing process into the current OSPF routing process.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the current OSPF routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into an OSPF process.
subnets	(Optional) For redistributing routes into OSPF, scopes the redistribution for the specified protocol. If not used, only classful routes are redistributed.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Defaults

The following are the command defaults:

- **metric** *metric-value*: 0
- **metric-type** *type-value*: **2**
- **match**: **Internal**, **external 1**, **external 2**
- **tag** *tag-value*: 0

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	This command was modified to include the **rip** keyword.
8.0(2)	This command was modified to include the **eigrp** keyword.

Examples

This example shows how to redistribute static routes into the current OSPF process:

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute static
```

Related Commands

Command	Description
redistribute (RIP)	Redistributes routes into the RIP routing process.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

redistribute (RIP)

To redistribute routes from another routing domain into the RIP routing process, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

no redistribute {{**ospf** *pid* [**match** {**internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**]}]} | **static** | **connected** | **eigrp** *as-number*} [**metric** {*metric_value* | **transparent**}] [**route-map** *map_name*]

Syntax Description

connected	Specifies redistributing a network connected to an interface into the RIP routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the RIP routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from OSPF to RIP.
metric {*metric_value* | **transparent**}	(Optional) Specifies the RIP metric value for the route being redistributed. Valid values for *metric_value* are from 0 to 16. Setting the metric to **transparent** causes the current route metric to be used.
nssa-external *type*	Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the RIP routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the RIP routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into a RIP process.

Defaults

The following are the command defaults:

- **metric** *metric-value*: 0
- **match**: **Internal**, **external 1**, **external 2**

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	This command was modified to include the **eigrp** keyword.

Examples

This example shows how to redistribute static routes into the current RIP process:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# redistribute static metric 2
```

Related Commands

Command	Description
redistribute (EIGRP)	Redistributes routes from other routing domains into EIGRP.
redistribute (OSPF)	Redistributes routes from other routing domains into OSPF.
router rip	Enables the RIP routing process and enters router configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redundant-interface

To set which member interface of a redundant interface is active, use the **redundant-interface** command in privileged EXEC mode.

redundant-interface redundant*number* **active-member** *physical_interface*

Syntax Description

active-member *physical_interface*	Sets the active member. See the **interface** command for accepted values. Both member interfaces must be the same physical type.
redundant*number*	Specifies the redundant interface ID, such as **redundant1**.

Defaults

By default, the active interface is the first member interface listed in the configuration, if it is available.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To view which interface is active, enter the following command:

```
hostname# show interface redundantnumber detail | grep Member
```

For example:

```
hostname# show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

Examples

The following example creates a redundant interface. By default, gigabitethernet 0/0 is active because it is first in the configuration. The redundant-interface command sets gigabitethernet 0/1 as the active interface.

```
hostname(config-if)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1

hostname(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
member-interface	Assigns a member interface to a redundant interface pair.
show interface	Displays the runtime status and statistics of interfaces.

regex

To create a regular expression to match text, use the **regex** command in global configuration mode. To delete a regular expression, use the **no** form of this command.

regex *name regular_expression*

no regex *name* [*regular_expression*]

Syntax Description

name	Specifies the regular expression name, up to 40 characters in length.
regular_expression	Specifies the regular expression up to 100 characters in length. See "Usage Guidelines" for a list of metacharacters you can use in the regular expression.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **regex** command can be used for various features that require text matching. For example, you can configure special actions for application inspection using Modular Policy Framework using an *inspection policy map* (see the **policy map type inspect** command). In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map (see the **class-map type regex** command).

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.

Note As an optimization, the security appliance searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like "http://", be sure to search for "http:/" instead.

Table 23-1 lists the metacharacters that have special meanings.

Table 23-1 regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp***)**	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*****	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x***}** or **{***x***,}**	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc***]**	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc***]**	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a-c***]**	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **" test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.

Table 23-1 regex Metacharacters (continued)

Character	Description	Notes
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

To test a regular expression to make sure it matches what you think it will match, enter the **test regex** command.

The regular expression performance impact is determined by two main factors:

- The length of text that needs to be searched for a regular expression match.

  The regular expression engine has only a small impact to the security appliance performance when the search length is small.

- The number of regular expression chained tables that need to be searched for a regular expression match.

How the Search Length Impacts Performance

When you configure a regular expression search, every byte of the searched text is usually examined against a regular expression database to find a match. The longer the searched text is, the longer the search time will be. Below is a performance test case which illustrates this phenomenon.

- An HTTP transaction includes one 300-byte long GET request and one 3250-byte long response.
- 445 regular expressions for URI search and 34 regular expressions for request body search.
- 55 regular expressions for response body search.

When a policy is configured to search the URI and the body in the HTTP GET request only, the throughput is:

- 420 mbps when the corresponding regular expression database is not searched.
- 413 mbps when the corresponding regular expression database is searched (this demonstrates a relatively small overhead of using regular expression).

But when a policy is configured to also search the whole HTTP response body, the throughput drops down to 145 mbps because of the long response body (3250 bytes) search.

Following is a list of factors that will increase the length of text for a regular expression search:

- A regular expression search is configured on multiple, different protocol fields. For example, in HTTP inspection, if only URI is configured for a regular expression match, then only the URI field is searched for a regular expression match, and the search length is then limited to the URI length. But if additional protocol fields are also configured for a regular expression match, such as Headers, Body, and so on, then the search length will increase to include the header length and body length.
- The field to be searched is long. For example, if the URI is configured for a regular expression search, then a long URI in a GET request will have a long search length. Also, currently the HTTP body search length is limited by default to 200 bytes. If, however, a policy is configured to search the body, and the body search length is changed to 5000 bytes, then there will be severe impact on the performance because of the long body search.

How the Number of Chained Regular Expression Tables Impact Performance

Currently, all regular expressions that are configured for the same protocol field, such as all regular expressions for URI, are built into a database consisting of one or more regular expression chained tables. The number of tables is determined by the total memory required and the availability of memory at the time the tables are built. A regular expression database will be split into multiple tables under any of the following conditions:

- When the total memory required is greater than 32 MB since the maximum table size is limited to 32 MB.
- When the size of the largest contiguous memory is not sufficient to build a complete regular expression database, then smaller but multiple tables will be built to accommodate all the regular expressions. Note that the degree of memory fragmentation varies depending on many factors that are interrelated and are almost impossible to predict the level of fragmentation.

With multiple chained tables, each table must be searched for regular expression matches and hence the search time increases in proportion to the number of tables that are searched.

Certain types of regular expressions tend to increase the table size significantly. It is prudent to design regular expressions in a way to avoid wildcard and repeating factors if possible. See Table 23-1 for a description of the following metacharacters:

- Regular expressions with wildcard type of specifications:
  - Dot (.)
- Various character classes that match any character in a class:
  - [^a-z]
  - [a-z]
  - [abc]]
- Regular expressions with repeating type of specifications:
  - *
  - +
  - {n,}
- Combination of the wild-card and repeating types of regular expressions can increase the table size dramatically, for examples:
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*

  - .*123.* (This should not be done because this is equivalent to matching "123").

The following examples illustrate how memory consumptions are different for regular expressions with and without wildcards and repetition.

- Database size for the following 4 regular expressions is 958,464 bytes.

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- Database size for the following 4 regular expressions is only 10240 bytes.

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

A large number of regular expressions will increase the total memory that is needed for the regular expression database and hence increases the probabilities of more tables if memory is fragmented. Following are examples of memory consumptions for different numbers of regular expressions:

- 100 sample URIs: 3,079,168 bytes
- 200 sample URIs: 7,156,224 bytes
- 500 sample URIs: 11,198,971 bytes

Note The maximum number of regular expressions per context is 2048.

The **debug menu regex 40 10** command can be used to display how many chained tables there are in each regex database.

Examples

The following example creates two regular expressions for use in an inspection policy map:

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

Related Commands

Command	Description
class-map type inspect	Creates ain inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
class-map type regex	Creates a regular expression class map.
test regex	Tests a regular expression.

reload

To reboot and reload the configuration, use the **reload** command in privileged EXEC mode.

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm***]** [**max-hold-time** [*hh*:]*mm***]** [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

Syntax Description

at *hh*:*mm*	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 hours.
cancel	(Optional) Cancels a scheduled reload.
day	(Optional) Number of the day in the range from 1 to 31.
in [*hh*:]*mm*]	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must occur within 24 hours.
max-hold-time [*hh*:]*mm*	(Optional) Specifies the maximum hold time the security appliance waits to notify other subsystems before a shutdown or reboot. After this time elapses, a quick (forced) shutdown/reboot occurs.
month	(Optional) Specifies the name of the month. Enter enough characters to create a unique string for the name of the month. For example, "Ju" is not unique because it could represent June or July, but "Jul" is unique because no other month beginning with those exact three letters.
noconfirm	(Optional) Permits the security appliance to reload without user confirmation.
quick	(Optional) Forces a quick reload, without notifying or properly shutting down all the subsystems.
reason *text*	(Optional) Specifies the reason for the reload, 1 to 255 characters. The reason text is sent to all open IPSec VPN client, terminal, console, telnet, SSH, and ASDM connections/sessions. **Note** Some applications, like isakmp, require additional configuration to send the reason text to IPSec VPN Clients. Refer to the appropriate section in the software configuration documentation for more information.
save-config	(Optional) Saves the running configuration to memory before shutting down. If you do not enter the **save-config** keyword, any configuration changes that have not been saved will be lost after the reload.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was modified to add the following new arguments and keywords: *day*, *hh*, *mm*, *month*, **quick**, **save-config**, and *text*.

Usage Guidelines

The command lets you reboot the security appliance and reload the configuration from Flash.

By default, the **reload** command is interactive. The security appliance first checks whether the configuration has been modified but not saved. If so, the security appliance prompts you to save the configuration. In multiple context mode, the security appliance prompts for each context with an unsaved configuration. If you specify the **save-config** parameter, the configuration is saved without prompting you. The security appliance then prompts you to confirm that you really want to reload the system. Only a response of **y** or pressing the **Enter** key causes a reload. Upon confirmation, the security appliance starts or schedules the reload process, depending upon whether you have specified a delay parameter (**in** or **at**).

By default, the reload process operates in "graceful" (also known as "nice") mode. All registered subsystems are notified when a reboot is about to occur, allowing these subsystems to shut down properly before the reboot. To avoid waiting until for such a shutdown to occur, specify the **max-hold-time** parameter to specify a maximum time to wait. Alternatively, you can use the **quick** parameter to force the reload process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

You can force the **reload** command to operate noninteractively by specifying the **noconfirm** parameter. In this case, the security appliance does not check for an unsaved configuration unless you have specified the **save-config** parameter. The security appliance does not prompt the user for confirmation before rebooting the system. It starts or schedules the reload process immediately, unless you have specified a delay parameter, although you can specify the **max-hold-time** or **quick** parameters to control the behavior or the reload process.

Use **reload cancel** to cancel a scheduled reload. You cannot cancel a reload that is already in progress.

Note Configuration changes that are not written to the Flash partition are lost after a reload. Before rebooting, enter the **write memory** command to store the current configuration in the Flash partition.

Examples

This example shows how to reboot and reload the configuration:

```
hostname# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

Related Commands

Command	Description
show reload	Displays the reload status of the security appliance.

remote-access threshold session-threshold-exceeded

To set threshold values, use the **remote-access threshold** command in global configuration mode. To remove threshold values, use the **no** version of this command. This command specifies the number of active remote access sessions, at which point the security appliance sends traps.

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

Syntax Description

threshold-value	Specifies an integer less than or equal to the session limit the security appliance supports.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0 (1)	This command was introduced.

Examples

The following example shows how to set a threshold value of 1500:

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

Related Commands

Command	Description
snmp-server enable trap remote-access	Enables threshold trapping.

rename

To rename a file or a directory from the source filename to the destination filename, use the **rename** command in privileged EXEC mode.

rename ***[/noconfirm] [*****disk0: | disk1: | flash:*****]*** ***source-path*** **[disk0: | disk1: | flash:*****]*** ***destination-path***

Syntax Description

/noconfirm	(Optional) Suppresses the confirmation prompt.
destination-path	Specifies the path of the destination file.
disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
source-path	Specifies the path of the source file.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **rename flash: flash:** command prompts you to enter a source and destination filename.

You cannot rename a file or directory across file systems.

For example:

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

Examples

The following example shows how to rename a file named “test” to “test1”:

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

Related Commands

Command	Description
mkdir	Creates a new directory.
rmdir	Removes a directory.
show file	Displays information about the file system.

rename (class-map)

To rename a class map, enter the **rename** command in class-map configuration mode.

rename *new_name*

Syntax Description

new_name	Specifies the new name of the class map, up to 40 characters in length. The name "class-default" is reserved.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to rename a class map from test to test2:

```
hostname(config)# class-map test
hostname(config-cmap)# rename test2
```

Related Commands

Command	Description
class-map	Creates a class map.

renewal-reminder

To specify the number of days prior to local Certificate Authority (CA) certificate expiration that an initial reminder to re-enroll is sent to certificate owners, use the **renewal-reminder** command in CA server configuration mode. To reset the time to the default of 14 days, use the **no** form of this command.

renewal-reminder *time*

no renewal-reminder

Syntax Description

time	Specifies the time in days prior to the expiration of an issued certificate that the certificate owner is first reminded to re-enroll. Valid values range from 1 to 90 days.

Defaults

By default, the CA server sends an expiration notice and reminder to re-enroll 14 days prior to certificate expiration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

There are three reminders in all: one at the renewal-reminder time prior to certificate expiration, a second at (expiration time + otp expiration) - renewal-reminder time/2, and a third at (expiration time + otp expiration) - renewal-reminder/4.

An e-mail is sent automatically to the certificate owner for each of the three reminders, if an e-mail address is specified in the user database. If no e-mail address exists, a syslog message is generated to alert the administrator of the renewal.

Examples

The following example specifies that the security appliance send an expiration notice to users 7 days prior to certificate expiration:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# renewal-reminder 7
hostname(config-ca-server)#
```

The following example resets the expiration notice time to the default of 14 days prior to certificate expiration:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no renewal-reminder
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
lifetime	Specifies the lifetimes of the CA certificate, all issued certificates, and the CRL.
show crypto ca server	Displays the configuration details of the local CA server.

replication http

To enable HTTP connection replication for the failover group, use the **replication http** command in failover group configuration mode. To disable HTTP connection replication, use the **no** form of this command.

replication http

no replication http

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

By default, the security appliance does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

This command is available for Active/Active failover only. It provides the same functionality as the **failover replication http** command for Active/Standby failover, except for failover groups in Active/Active failover configurations.

Examples

The following example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover replication http	Configures stateful failover to replicate HTTP connections.

request-command deny

To disallow specific commands within FTP requests, use the **request-command deny** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the **no** form of this command.

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

Syntax Description

appe	Disallows the command that appends to a file.
cdup	Disallows the command that changes to the parent directory of the current working directory.
dele	Disallows the command that deletes a file on the server.
get	Disallows the client command for retrieving a file from the server.
help	Disallows the command that provides help information.
mkd	Disallows the command that makes a directory on the server.
put	Disallows the client command for sending a file to the server.
rmd	Disallows the command that deletes a directory on the server.
rnfr	Disallows the command that specifies rename-from filename.
rnto	Disallows the command that specifies rename-to filename.
site	Disallows the command that is specific to the server system. Usually used for remote administration.
stou	Disallows the command that stores a file using a unique file name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
FTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used for controlling the commands allowed within FTP requests traversing the security appliance when using strict FTP inspection.

Examples

The following example causes the security appliance to drop FTP requests containing **stor**, **stou**, or **appe** commands:

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.

request-data-size

To set the size of the payload in the SLA operation request packets, use the **request-data-size** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

request-data-size *bytes*

no request-data-size

Syntax Description

bytes	The size, in bytes, of the request packet payload. Valid values are from 0 to 16384. The minimum value depends upon the protocol used. For echo types, the minimum value is 28 bytes. Do not set this value higher than the maximum allowed by the protocol or the PMTU. **Note** The security appliance adds an 8 byte timestamp to the payload, so the actual payload is *bytes* + 8.

Defaults

The default *bytes* is 28.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

For reachability, it may be necessary to increase the default data size to detect PMTU changes between the source and the target. Low PMTU will likely affect session performance and, if detected, may indicate that the secondary path be used.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes and the number of echo requests sent during an SLA operation to 5.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
```

```
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

request-queue

To specify the maximum number of GTP requests that will be queued waiting for a response, use the **request-queue** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to return this number to the default of 200.

request-queue *max_requests*

no request-queue *max_requests*

Syntax Description

max_requests	The maximum number of GTP requests that will be queued waiting for a response. The range values is 1 to 4294967295.

Defaults

The *max_requests* default is 200.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **gtp request-queue** command specifies the maximum number of GTP requests that are queued waiting for a response. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

Examples

The following example specifies a maximum request queue size of 300 bytes:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.

Commands	Description
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

request-timeout

To configure the number of seconds before a failed SSO authentication attempt times out, use the **request-timeout** command in webvpn configuration mode.

To return to the default value, use the **no** form of this command.

request-timeout *seconds*

no request-timeout

Syntax Description

seconds	The number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds. Fractions are not supported.

Defaults

The default value for this command is 5 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports SiteMinder and SAML POST type SSO servers.

This command applies to both types of SSO Servers.

Once you have configured the security appliance to support SSO authentication, you have the option to adjust two timeout parameters:

- The number of seconds before a failed SSO authentication attempt times out using the **request-timeout** command.
- The number of times the security appliance retries a failed SSO authentication attempt. (See the **max-retry-attempts** command.)

Examples

The following example, entered in webvpn-config-sso-siteminder mode, configures an authentication timeout at ten seconds for the SiteMinder type SSO server, “example”:

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# request-timeout 10
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

reserve-port-protect

To restrict usage on the reserve port during media negotiation, use the **reserve-port-protect** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

reserve-port-protect

no reserve-port-protect

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows how to protect the reserve port in an RTSP inspection policy map:

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# reserve-port-protect
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

reserved-bits

To clear reserved bits in the TCP header, or drop packets with reserved bits set, use the **reserved-bits** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

Syntax Description

allow	Allows packet with the reserved bits in the TCP header.
clear	Clears the reserved bits in the TCP header and allows the packet.
drop	Drops the packet with the reserved bits in the TCP header.

Defaults

The reserved bits are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **reserved-bits** command in tcp-map configuration mode to remove ambiguity as to how packets with reserved bits are handled by the end host, which may lead to desynchronizing the security appliance. You can choose to clear the reserved bits in the TCP header or even drop packets with the reserved bits set.

Examples

The following example shows how to clear packets on all TCP flows with the reserved bit set:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
```

```
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

reset

When using the Modular Policy Framework, drop packets, close the connection, and send a TCP reset for traffic that matches a **match** command or class map by using the **reset** command in match or class configuration mode. This reset action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the **no** form of this command.

reset [**log**]

no reset [**log**]

Syntax Description

log	Logs the match. The system log message number depends on the application.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **reset** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you reset a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to reset the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. You can configure both the **reset** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is reset for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

Examples

The following example resets the connection and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

Related Commands

Commands	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
policy-map type inspect	Defines special actions for application inspection.
show running-config policy-map	Display all current policy map configurations.

retries

To specify the number of times to retry the list of DNS servers when the security appliance does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

retries *number*

no retries [*number*]

Syntax Description

number	Specifies the number of retries, from 0 through 10. The default is 2.

Defaults

The default number of retries is 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Add DNS servers using the **name-server** command.

This command replaces the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The security appliance tries each server only once.

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns retries 0
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters the dns server-group mode.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

retry-interval

To configure the amount of time between retry attempts for a particular AAA server designated in a prior aaa-server host command, use the **retry-interval** command in AAA-server host mode. To reset the retry interval to the default value, use the **no** form of this command.

retry-interval *seconds*

no retry-interval

Syntax Description

seconds	Specify the retry interval (1-10 seconds) for the request. This is the time the security appliance waits before retrying a connection request.

Defaults

The default retry interval is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
AAA-server host	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the security appliance waits between connection attempts. Use the **timeout** command to specify the length of time during which the security appliance attempts to make a connection to a AAA server.

Examples

The following examples show the **retry-interval** command in context.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.

clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol
timeout	Specifies the length of time during which the security appliance attempts to make a connection to a AAA server.

reval-period

To specify the interval between each successful posture validation in a NAC Framework session, use the **reval-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC Framework policy, use the **no** form of this command.

reval-period *seconds*

no reval-period [*seconds***]**

Syntax Description

seconds	Number of seconds between each successful posture validation. The range is 300 to 86400.

Defaults

The default value is 36000.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	"nac-" removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance starts the revalidation timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The security appliance maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation.

Examples

The following example changes the revalidation timer to 86400 seconds:

```
hostname(config-nac-policy-nac-framework)# reval-period 86400
hostname(config-nac-policy-nac-framework)
```

The following example removes the revalidation timer from the NAC policy:

```
hostname(config-nac-policy-nac-framework)# no reval-period
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
`eou timeout`	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
`sq-period`	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
`nac-policy`	Creates and accesses a Cisco NAC policy, and specifies its type.
`debug nac`	Enables logging of NAC Framework events.
`eou revalidate`	Forces immediate posture revalidation of one or more NAC Framework sessions.

revert webvpn all

To remove all web-related data (customization, plug-in, translation table, URL list, and web content) from the security appliance flash memory, enter the **revert webvpn all** command in privileged EXEC mode.

revert webvpn all

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn all** command to disable and remove all web-related information (customization, plug-in, translation table, URL list, and web content) from the flash memory of the security appliance. Removal of all web-related data returns default settings when applicable.

Examples

The following command removes all of the web-related configuration data from the security appliance:

```
hostname# revert webvpn all
hostname
```

Related Commands

Command	Description
show import webvpn (*option*)	Displays various imported WebVPN data and plug-ins. currently present in flash memory on the security appliance.

revert webvpn customization

To remove a customization object from the security appliance cache memory, enter the **revert webvpn customization** command in privileged EXEC mode.

revert webvpn customization *name*

Syntax Description

name	Specifies the name of the customization object to be deleted.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn customization** command to remove Clientless SSL VPN support for the specified customization and to remove it from the cache memory on the security appliance. Removal of a customization object returns default settings when applicable. A customization object contains the configuration parameters for a specific, named portal page.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.

Note Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file before you upgrade to Version 8.0.

Examples

The following command removes the customization object named GroupB:

```
hostname# revert webvpn customization groupb
hostname
```

Related Commands

Command	Description
`customization`	Specifies the customization object to use for a tunnel-group, group, or user.
`export customization`	Exports a customization object.
`import customization`	Installs a customization object.
`revert webvpn all`	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
`show webvpn customization`	Displays the current customization objects present on the flash device of the security appliance.

revert webvpn plug-in protocol

To remove a plug-in from the flash device of the security appliance, enter the **revert webvpn plug-in protocol** command in privileged EXEC mode.

revert plug-in protocol *protocol*

Syntax Description

protocol	Enter one of the following strings: • **rdp** The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services. • **ssh** The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer. • **vnc** The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn plug-in protocol** command to disable and remove Clientless SSL VPN support for the specified Java-based client application, as well as to remove it from the flash drive of the security appliance.

Examples

The following command removes support for RDP:

```
hostname# revert webvpn plug-in protocol rdp
hostname
```

Related Commands

Command	Description
`import webvpn plug-in protocol`	Copies the specified plug-in from a URL to the flash device of the security appliance. Clientless SSL VPN automatically supports the use of the Java-based client application for future sessions when you issue this command.
`show import webvpn plug-in`	Lists the plug-ins present on the flash device of the security appliance.

revert webvpn translation-table

To remove a translation table from the security appliance flash memory, enter the **revert webvpn translation-table** command in privileged EXEC mode.

revert webvpn translation-table *translationdomain language*

Syntax Description

translationdomain	Available translation domains: • AnyConnect • PortForwarder • Banners • CSD • Customization • URL List • (Translations of messages from RDP, SSH, and VNC plug-ins.)
language	Specifies the character-encoding method to be deleted.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn translation-table** command to disable and remove an imported translation table and to remove it from the flash memory on the security appliance. Removal of a translation table returns default settings when applicable.

Examples

The following command removes the AnyConnect translation table, Dutch:

```
hostname# revert webvpn translation-table anyconnect dutch
hostname
```

Related Commands

Command	Description
`revert webvpn all`	Removes all webvpn-related data (customization, plug-in, translation table, URL-list, and web content) .
`show webvpn translation-table`	Displays the current translation tables currently present on the flash device of the security appliance.

revert webvpn url-list

To remove a URL list from the security appliance, enter the **revert webvpn url-list** command in privileged EXEC mode.

revert webvpn url-list template *name*

Syntax Description

template *name*	Specifies the name of a URL list.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn url-list** command to disable and remove a current URL list from the flash drive of the security appliance. Removal of a url-list returns default settings when applicable.

The template argument used with the **revert webvpn url-list** command specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Examples

The following command removes the URL list, servers2:

```
hostname# revert webvpn url-list servers2
hostname
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content) .
show running-configuration url-list	Displays the current set of configured URL list commands.
url-list (WebVPN mode)	Applies a list of WebVPN servers and URLs to a particular user or group policy.

revert webvpn webcontent

To remove a specified web object from a location in the security appliance flash memory, enter the **revert webvpn webcontent** command in privileged EXEC mode.

revert webvpn webcontent *filename*

Syntax Description

filename	Specifies the name of the flash memory file with the web content to be deleted.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **revert webvpn content** command to disable and remove a file containing the web content and to remove it from the flash memory of the security appliance. Removal of web content returns default settings when applicable.

Examples

The following command removes the web content file, ABCLogo, from the security appliance flash memory:

```
hostname# revert webvpn webcontent abclogo
hostname
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn webcontent	Displays the web content currently present in flash memory on the security appliance.

revocation-check

To set one or more methods for revocation checking, use the **revocation-check** command in crypto ca trustpoint mode. The security appliance tries the methods in the order that you configure them, trying the second and third methods only if the previous method returns an error (for example, server down), as opposed to finding the status as revoked.

You can set a revocation checking method in the client certificate validating trustpoint and also configure no revocation checking (**revocation-check none)** in the responder certificate validating trustpoint. The **match certificate** command documentation includes step-by-step configuration example.

To restore the default revocation checking method, which is *none*, use the **no** version of this command.

revocation-check {[**crl**] [**none**] [**ocsp]}**

no revocation-check

Syntax Description

crl	Specifies that the security appliance should use CRL as the revocation checking method.
none	Specifies that the security appliance should interpret the certificate status as valid, even if all methods return an error.
ocsp	Specifies that the security appliance should use OCSP as the revocation checking method.

Defaults

The default value is *none*.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
crypto ca trustpoint mode	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced. The following permutations replace previous commands: • **revocation-check crl none** replaces **crl optional** • **revocation-check crl** replaces **crl required** • **revocation-check none** replaces **crl nocheck**

Usage Guidelines

The signer of the OCSP response is usually the OCSP server (responder) certificate. After receiving the response, devices try to verify the responder certificate.

Normally a CA sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of compromising its security. The CA includes an ocsp-no-check extension in the responder certificate that indicates it does not need revocation status checking. But if this extension is not present, the device tries to check the certificate's revocation status using the revocation methods you configure for the trustpoint with this **revocation-check** command.The OCSP responder certificate must be verifiable if it does not have an ocsp-no-check extension since the OCSP revocation check fails unless you also set the *none* option to ignore the status check.

Examples

The following example shows how to set revocation methods of OCSP and CRL, in that order, for the trustpoint called newtrust.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp crl
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca trustpoint mode. Use this command in global configuration mode.
match certificate	Configures an OCSP override rule,
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.

rewrite

To disable content rewriting a particular application or type of traffic over a WebVPN connection, use the **rewrite** command in webvpn mode. To eliminate a rewrite rule, use the **no** form of this command with the rule number, which uniquely identifies the rule. To eliminate all rewriting rules, use the **no** form of the command without the rule number.

By default, the security appliance rewrites, or transforms, all WebVPN traffic.

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

Syntax Description

disable	Defines this rewrite rule as a rule that disables content rewriting for the specified traffic. When you disable content rewriting, traffic does not go through the security appliance.
enable	Defines this rewrite rule as a rule that enables content rewriting for the specified traffic.
integer	Sets the order of the rule among all of the configured rules. The range is 1-65534.
name	(Optional) Identifies the name of the application or resource to which the rule applies.
order	Defines the order in which the security appliance applies the rule.
resource-mask	Identifies the application or resource for the rule.
resource name	(Optional) Specifies the application or resource to which the rule applies. Maximum 128 bytes.
string	Specifies the name of the application or resource to match that can contain a regular expression. You can use the following wildcards: Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 300 bytes.

Defaults

The default is to rewrite everything.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The security appliance performs content rewriting for applications to insure that they render correctly over WebVPN connections. Some applications do not require this processing, such as external public websites. For these applications, you might choose to turn off content rewriting.

You can turn off content rewriting selectively by using the rewrite command with the disable option to let users browse specific sites directly without going through the security appliance. This is similar to split-tunneling in IPSec VPN connections.

You can use this command multiple times. The order in which you configure entries is important because the security appliance searches rewrite rules by order number and applies the first rule that matches.

Examples

The following example shows how to configure a rewrite rule, order number of 1, that turns off content rewriting for URLS from cisco.com domains:

```
hostname(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
proxy-bypass	Configures minimal content rewriting for a particular application.

re-xauth

To require that IPSec users reauthenticate on IKE rekey, issue the **re-xauth enable** command in group-policy configuration mode. To disable user reauthentication on IKE rekey, use the **re-xauth disable** command.

To remove the re-xauth attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for reauthentication on IKE rekey from another group policy.

re-xauth {**enable** [**extended**] | **disable}**

no re-xauth

Syntax Description

disable	Disables reauthentication on IKE rekey
enable	Enables reauthentication on IKE rekey
extended	Extends the time allowed for reentering authentication credentials until the maximum lifetime of the configured SA.

Defaults

Reauthentication on IKE rekey is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group policy	•	—	•	—	—

Command History

Release	Modification
8.0.4	The **extended** keyword was added.
7.0(1)	This command was introduced.

Usage Guidelines

Reauthentication on IKE rekey applies only to IPSec connections.

If you enable reauthentication on IKE rekey, the security appliance prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates. Use the **extended** keyword to allow users to reenter authentication credentials until the maximum lifetime of the configured SA.

To check the configured rekey interval, in monitoring mode, issue the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data.

Note The reauthentication fails if there is no user at the other end of the connection.

Examples

The following example shows how to enable reauthentication on rekey for the group policy named FirstGroup:

```
hostname(config) #group-policy FirstGroup attributes
hostname(config-group-policy)# re-xauth enable
```

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

rip send version {[**1**] [**2**]}

no rip send version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance sends RIP Version 1 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to send and receive RIP Version 1 and 2 packets on the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.
version	Specifies the version of RIP used globally by the security appliance.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

version {[**1**] [**2**]}

no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance accepts Version 1 and Version 2 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to receive RIP Version 1 and 2 packets the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.
version	Specifies the version of RIP used globally by the security appliance.

rip authentication mode

To specify the type of authentication used in RIP Version 2 packets, use the **rip authentication mode** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

rip authentication mode {**text** | **md5**}

no rip authentication mode

Syntax Description

md5	Uses MD5 for RIP message authentication.
text	Uses clear text for RIP message authentication (not recommended).

Defaults

Clear text authentication is used by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

Command	Description
rip authentication key	Enables RIP Version 2 authentication and specifies the authentication key.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the security appliance.

rip authentication key

To enable authentication of RIP Version 2 packets and specify the authentication key, use the **rip authentication key** command in interface configuration mode. To disable RIP Version 2 authentication, use the **no** form of this command.

rip authentication key *key* **key_id** *key_id*

no rip authentication key

Syntax Description

key	Key to authenticate RIP updates. The key can contain up to 16 characters.
key_id	Key identification value; valid values range from 1 to 255.

Defaults

RIP authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates. When you enable neighbor authentication, you must ensure that the *key* and *key_id* arguments are the same as those used by neighbor devices that provide RIP version 2 updates. The *key* is a text string of up to 16 characters.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

Command	Description
rip authentication mode	Specifies the type of authentication used in RIP Version 2 packets.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the security appliance.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

version {[**1**] [**2**]}

no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance accepts Version 1 and Version 2 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to receive RIP Version 1 and 2 packets the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.
version	Specifies the version of RIP used globally by the security appliance.

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

rip send version {[**1**] [**2**]}

no rip send version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance sends RIP Version 1 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to send and receive RIP Version 1 and 2 packets on the specified interface:

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.
version	Specifies the version of RIP used globally by the security appliance.

rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

rmdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
disk0*:*	(Optional) Specifies the nonremovable internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the removable external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the nonremovable internal Flash, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
path	(Optional) The absolute or relative path of the directory to remove.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If the directory is not empty, the **rmdir** command fails.

Examples

This example shows how to remove an existing directory named “test”:

```
hostname# rmdir test
```

Related Commands

Command	Description
dir	Displays the directory contents.
mkdir	Creates a new directory.
pwd	Displays the current working directory.
show file	Displays information about the file system.

route

To enter a static or default route for the specified interface, use the **route** command in global configuration mode. Use the **no** form of this command to remove routes from the specified interface.

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]

Syntax Description

gateway_ip	Specifies the IP address of the gateway router (the next-hop address for this route). **Note** The *gateway_ip* argument is optional in transparent mode.
interface_name	Internal or external network interface name through which the traffic is routed.
ip_address	Internal or external network IP address.
metric	(Optional) The administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
netmask	Specifies a network mask to apply to *ip_address*.
track *number*	(Optional) Associates a tracking entry with this route. Valid values are from 1 to 500. **Note** The **track** option is only available in single, routed mode.
tunneled	Specifies route as the default tunnel gateway for VPN traffic.

Defaults

The *metric* default is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	The **track** *number* value was added.

Usage Guidelines

Use the **route** command to enter a default or static route for an interface. To enter a default route, set *ip_address* and *netmask* to **0.0.0.0,** or use the shortened form of **0**. All routes that are entered using the **route** command are stored in the configuration when it is saved.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the security appliance that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled** option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route. Doing so causes the session to fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with tunneled routes. These inspection engines ignore the tunneled route.

You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

Create static routes to access networks that are connected outside a router on any interface. For example, the security appliance sends all packets that are destined to the 192.168.42.0 network through the 192.168.1.5 router with this static **route** command.

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

Once you enter the IP address for each interface, the security appliance creates a CONNECT route in the route table. This entry is not deleted when you use the **clear route** or **clear configure route** commands.

If the **route** command uses the IP address from one of the interfaces on the security appliance as the gateway IP address, the security appliance will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address.

Examples

The following example shows how to specify one default **route** command for an outside interface:

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

The following example shows how to add these static **route** commands to provide access to the networks:

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

The following example uses an SLA operation to install a default route to the 10.1.1.1 gateway on the outside interface. The SLA operation monitors the availability of that gateway.If the SLA operation fails, then the backup route on the dmz interface is used.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
hostname(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

Related Commands

Command	Description
clear configure route	Removes statically configured **route** commands.
clear route	Removes routes learned through dynamic routing protocols such as RIP.
show route	Displays route information.
show running-config route	Displays configured routes.

route-map

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** command in global configuration mode. To delete a map, use the **no** form of this command.

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

Syntax Description

deny	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
map_tag	Text for the route map tag; the text can be up to 57 characters in length.
permit	(Optional) Specifies that if the match criteria is met for this route map, the route is redistributed as controlled by the set actions.
seq_num	(Optional) Route map sequence number; valid values are from 0 to 65535. Indicates the position that a new route map will have in the list of route maps already configured with the same name.

Defaults

The defaults are as follows:

- **permit.**
- If you do not specify a *seq_num*, a *seq_num* of 10 is assigned to the first route map.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **route-map** command lets you redistribute routes.

The **route-map** global configuration command `and the **match** and **set** configuration commands define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria that are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. You can enter the **match** commands in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** form of the **match** commands removes the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. You specify the destination routing protocol with the **router ospf** global configuration command. You specify the source routing protocol with the **redistribute** router configuration command.

When you pass routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored; the route is not advertised for outbound route maps and is not accepted for inbound route maps. To modify only some data, you must configure a second route map section with an explicit match specified.

The *seq_number* argument is as follows:

1. If you do not define an entry with the supplied tag, an entry is created with the *seq_number* argument set to 10.
2. If you define only one entry with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *seq_number* argument of this entry is unchanged.
3. If you define more than one entry with the supplied tag, an error message is printed to indicate that the *seq_number* argument is required.

If the **no route-map** *map-tag* command is specified (with no *seq-num* argument), the whole route map is deleted (all **route-map** entries with the same *map-tag* text).

If the match criteria are not met, and you specify the **permit** keyword, the next route map with the same *map_tag* is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

Examples

The following example shows how to configure a route map in OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
clear configure route-map	Removes the conditions for redistributing the routes from one routing protocol into another routing protocol.
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
router ospf	Starts and configures an ospf routing process.
set metric	Specifies the metric value in the destination routing protocol for a route map.
show running-config route-map	Displays the information about the route map configuration.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To reset OSPF to use the previous router ID behavior, use the **no** form of this command.

router-id *addr*

no router-id [*addr*]

Syntax Description

addr	Router ID in IP address format.

Defaults

If not specified, the highest-level IP address on the security appliance is used as the router ID.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.
8.0(2)	The processing order for this command was changed. The command is now processed before the **network** commands in an OSPF configuration.

Usage Guidelines

By default, the security appliance uses the highest-level IP address on an interface that is covered by a **network** command in the OSPF configuration. If the highest-level IP address is a private address, then that address is sent in hello packets and database definitions. To use a specific router ID, use the **router-id** command to specify a global address for the router ID.

Router IDs must be unique within an OSPF routing domain. If two routers in the same OSPF domain are using the same router ID, routing may not work correctly.

You should enter the **router-id** command before entering **network** commands in an OSPF configuration. This prevents possible conflicts with the default router ID generated by the security appliance. If you do have a conflict, you will receive the message:

```
ERROR: router-id addr in use by ospf process pid
```

To enter the conflicting ID, remove the **network** command that contains the IP address causing the conflict, enter the **router-id** command, and then re-enter the **network** command.

Examples

The following example sets the router ID to 192.168.1.1:

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.

router eigrp

To start an EIGRP routing process and configure parameters for that process, use the **router eigrp** command in global configuration mode. To disable EIGRP routing, use the **no** form of this command.

router eigrp *as-number*

no router eigrp *as-number*

Syntax Description

as-number	Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information. Valid values are from 1 to 65535.

Defaults

EIGRP routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **router eigrp** command creates an EIGRP routing process or enters router configuration mode for an existing EIGRP routing process. You can only create a single EIGRP routing process on the security appliance.

Use the following router configuration mode commands to configure the EIGRP routing processes:

- **auto-summary**—Enable/disable automatic route summarization.
- **default-information**—Enable/disable the reception and sending of default route information.
- **default-metric**—Define the default metrics for routes redistributed into the EIGRP routing process.
- **distance eigrp**—Configure the administrative distance for internal and external EIGRP routes.
- **distribute-list**—Filter the networks received and sent in routing updates.
- **eigrp log-neighbor-changes**—Enable/disable the logging of neighbor state changes.
- **eigrp log-neighbor-warnings**—Enable/disable the logging of neighbor warning messages.
- **eigrp router-id**—Creates a fixed router ID.
- **eigrp stub**—Configures the security appliance for stub EIGRP routing.
- **neighbor**—Statically define an EIGRP neighbor.

- **network**—Configure the networks that participate in the EIGRP routing process.
- **passive-interface**—Configure an interface to act as a passive interface.
- **redistribute**—Redistribute routes from other routing processes into EIGRP.

Use the following interface configuration mode commands to configure interface-specific EIGRP parameters:

- **authentication key eigrp**—Define the authentication key used for EIGRP message authentication.
- **authentication mode eigrp**—Define the authentication algorithm used for EIGRP message authentication.
- **delay**—Configure the delay metric for an interface.
- **hello-interval eigrp**—Change the interval at which EIGRP hello packets are sent out of an interface.
- **hold-time eigrp**—Change the hold time advertised by the security appliance.
- **split-horizon eigrp**—Enable/disable EIGRP split-horizon on an interface.
- **summary-address eigrp**—Manually define a summary address.

Examples

The following example shows how to enter the configuration mode for the EIGRP routing process with the autonomous system number 100:

```
hostname(config)# router eigrp 100
hostname(config-router)#
```

Related Commands

Command	Description
clear configure eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

router ospf *pid*

no router ospf *pid*

Syntax Description

pid	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The *pid* does not need to match the ID of OSPF processes on other routers.

Defaults

OSPF routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the security appliance. Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in router configuration mode.

When using the **no router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no router ospf** command terminates the OSPF routing process specified by its *pid*. You assign the *pid* locally on the security appliance. You must assign a unique value for each OSPF routing process.

The **router ospf** command is used with the following OSPF-specific commands to configure OSPF routing processes:

- **area**—Configures a regular OSPF area.
- **compatible rfc1583**—Restores the method used to calculate summary route costs per RFC 1583.
- **default-information originate**—Generates a default external route into an OSPF routing domain.
- **distance**—Defines the OSPF route administrative distances based on the route type.
- **ignore**—Suppresses the sending of syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets.

- **log-adj-changes**—Configures the router to send a syslog message when an OSPF neighbor goes up or down.
- **neighbor**—Specifies a neighbor router. Used to allow adjacency to be established over VPN tunnels.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain to another according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timers lsa-group-pacing**—OSPF LSA group pacing timer (interval between group of LSA being refreshed or max-aged).
- **timers spf**—Delay between receiving a change to the SPF calculation.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
hostname(config)# router ospf 5
hostname(config-router)#
```

Related Commands

Command	Description
clear configure router	Clears the OSPF router commands from the running configuration.
show running-config router ospf	Displays the OSPF router commands in the running configuration.

router rip

To start a RIP routing process and configure parameters for that process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

router rip

no router rip

Syntax Description

This command has no arguments or keywords.

Defaults

RIP routing is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **router rip** command is the global configuration command for configuring the RIP routing processes on the security appliance. You can only configure one RIP process on the security appliance. The **no router rip** command terminates the RIP routing process and removes all router configuration for that process.

When you enter the **router rip** command the command prompt changes to `hostname(config-router)#`, indicating that you are in router configuration mode.

The **router rip** command is used with the following router configuration commands to configure RIP routing processes:

- **auto-summary**—Enable/disable automatic summarization of routes.
- **default-information originate**—Distribute a default route.
- **distribute-list in**—Filter networks in incoming routing updates.
- **distribute-list out**—Filter networks in outgoing routing updates.
- **network**—Add/remove interfaces from the routing process.
- **passive-interface**—Set specific interfaces to passive mode.
- **redistribute**—Redistribute routes from other routing processes into the RIP routing process.
- **version**—Set the RIP protocol version used by the security appliance.

Additionally, you can use the following commands in interface configuration mode to configure RIP properties on a per-interface basis:

- **rip authentication key**—Set an authentication key.
- **rip authentication mode**—Set the type of authentication used by RIP Version 2.
- **rip send version**—Set the version of RIP used to send updates out of the interface. This overrides the version set in global router configuration mode, if any.
- **rip receive version**—Set the version of RIP accepted by the interface. This overrides the version set in global router configuration mode, if any.

RIP is not supported under transparent mode. By default, the security appliance denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through a security appliance operating in transparent mode you must define access list entries to permit this traffic. For example, to permit RIP version 2 traffic through the security appliance, create an access list entry such as `access-list myriplist extended permit ip any host 224.0.0.9`. To permit RIP version 1 broadcasts, create an access list entry such as `access-list myriplist extended permit udp any any eq rip`. Apply these access list entries to the appropriate interface using the **access-group** command.

You can enable both RIP and OSPF routing on the security appliance at the same time.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

Related Commands

Command	Description
clear configure router rip	Clears the RIP router commands from the running configuration.
show running-config router rip	Displays the RIP router commands in the running configuration.

rtp-conformance

To check RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP, use the **rtp-conformance** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

Syntax Description

enforce-payloadtype	Enforces payload type to be audio/video based on the signaling exchange.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to check RTP packets flowing on the pinholes for protocol conformance on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# rtp-conformance
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
debug rtp	Displays debug information and error messages for RTP packets associated with H.323 and SIP inspection.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

CHAPTER 24

same-security-traffic through show asdm sessions Commands

same-security-traffic

To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the **same-security-traffic** command in global configuration mode. To disable the same-security traffic, use the **no** form of this command.

same-security-traffic permit {**inter-interface | intra-interface**}

no same-security-traffic permit {**inter-interface | intra-interface**}

Syntax Description

inter-interface	Permits communication between different interfaces that have the same security level.
intra-interface	Permits communication in and out of the same interface.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **intra-interface** keyword now allows all traffic to enter and exit the same interface, and not just IPSec traffic.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) provides the following benefits:

- You can configure more than 101 communicating interfaces. If you use different levels for each interface, you can configure only one interface per level (0 to 100).
- You can allow traffic to flow freely between all same security interfaces without access lists.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed. This feature might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the security appliance is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the security appliance and then out again to the other spoke.

Note All traffic allowed by the **same-security-traffic intra-interface** command is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the security appliance.

Examples

The following example shows how to enable the same-security interface communication:

```
hostname(config)# same-security-traffic permit inter-interface
```

The following example shows how to enable traffic to enter and exit the same interface:

```
hostname(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
show running-config same-security-traffic	Displays the **same-security-traffic** configuration.

sasl-mechanism

To specify a SASL (Simple Authentication and Security Layer) mechanism for authenticating an LDAP client to an LDAP server, use the **sasl-mechanism** command in aaa-server host configuration mode. The SASL authentication mechanism options are **digest-md5** and **kerberos**.

To disable an authentication mechanism, use the **no** form of this command.

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

Note Because the security appliance serves as a client proxy to the LDAP server for VPN users, the LDAP client referred to here is the security appliance.

Syntax Description

digest-md5	The security appliance responds with an MD5 value computed from the username and password.
kerberos	The security appliance responds by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.
server-group-name	Specifies the Kerberos aaa-server group, up to 64 characters.

Defaults

No default behavior or values. The security appliance passes the authentication parameters to the LDAP server in plain text.

Note We recommend that you secure LDAP communications with SSL using the **ldap-over-ssl** command if you have not configured SASL.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to specify security appliance authentication to an LDAP server using SASL mechanisms.

Both the security appliance and the LDAP server can support multiple SASL authentication mechanisms. When negotiating SASL authentication, the security appliance retrieves the list of SASL mechanisms configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the security appliance and the server. The Kerberos mechanism is stronger than the Digest-MD5 mechanism. To illustrate, if both the LDAP server and the security appliance support both mechanisms, the security appliance selects Kerberos, the stronger of the mechanisms.

When disabling the SASL mechanisms, you must enter a separate **no** command for each mechanism you want to disable because they are configured independently. Mechanisms that you do not specifically disable remain in effect. For example, you must enter both of the following commands to disable both SASL mechanisms:

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

Examples

The following examples, entered in aaa-server host configuration mode, enable the SASL mechanisms for authentication to an LDAP server named ldapsvr1 with an IP address of 10.10.0.1. This example enables the SASL digest-md5 authentication mechanism:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
```

The following example enables the SASL Kerberos authentication mechanism and specifies kerb-servr1 as the Kerberos AAA server:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

sast

To specify the number of SAST certificates to create in the CTL record, use the **sast** command in ctl-file configuration mode. To set the number of SAST certificates in the CTL file back to the default value of 2, use the **no** form of this command.

sast *number_sasts*

no sast *number_sasts*

Syntax Description

number_sasts	Specifies the number of SAST keys to create. The default is 2. maximum allowed is 5.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

CTL files are signed by a System Administrator Security Token (SAST).

Because the Phone Proxy generates the CTL file, it needs to create the SAST key to sign the CTL file itself. This key can be generated on the security appliance. A SAST is created as a self-signed certificate.

Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.

Examples

The following example shows the use of the **sast** command to create 5 SAST certificates in the CTL file:

```
hostname(config-ctl-file)# sast 5
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

secondary

To give the secondary unit higher priority in a failover group, use the **secondary** command in failover group configuration mode. To restore the default, use the **no** form of this command.

secondary

no secondary

Syntax Description

This command has no arguments or keywords.

Defaults

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simulataneously (within a unit polltime). If one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
```

```
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
primary	Gives the primary unit a higher priority than the secondary unit.

secondary-color

To set a secondary color for the WebVPN login, home page, and file access page, use the **secondary-color** command in webvpn mode. To remove a color from the configuration and reset the default, use the **no** form of this command.

secondary-color [*color*]

no secondary-color

Syntax Description

color	(Optional) Specifies the color. You can use a comma separated RGB value, an HTML color value, or the name of the color if recognized in HTML. • RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others. • HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue. • Name length maximum is 32 characters

Defaults

The default secondary color is HTML #CCCCFF, a lavender shade.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The number of RGB values recommended for use is 216, many fewer than the mathematical possibilities. Many displays can handle only 256 colors, and 40 of those look differently on MACs and PCs. For best results, check published RGB tables. To find RGB tables online, enter RGB in a search engine.

Examples

The following example shows how to set an HTML color value of #5F9EAO, which is a teal shade:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

Related Commands

Command	Description
title-color	Sets a color for the WebVPN title bar on the login, home page, and file access page

secondary-text-color

To set the secondary text color for the WebVPN login, home page and file access page, use the **secondary-text-color** command in webvpn mode. To remove the color from the configuration and reset the default, use the **no** form of this command.

secondary-text-color [*black* | *white*]

no secondary-text-color

Syntax Description

auto	Chooses black or white based on the settings for the text-color command. That is, if the primary color is black, this value is white.
black	The default secondary text color is black.
white	You can change the text color to white.

Defaults

The default secondary text color is black.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set the secondary text color to white:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

Related Commands

Command	Description
text-color	Sets a color for text in the WebVPN title bar on the login, home page and file access page

secure-unit-authentication

To enable secure unit authentication, use the **secure-unit-authentication enable** command in group-policy configuration mode. To disable secure unit authentication, use the **secure-unit-authentication disable** command. To remove the secure unit authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for secure unit authentication from another group policy.

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel. With this feature enabled, the hardware client does not have a saved username and password.

Note With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

secure-unit-authentication {**enable** | **disable**}

no secure-unit-authentication

Syntax Description

disable	Disables secure unit authentication.
enable	Enables secure unit authentication.

Defaults

Secure unit authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware client(s) use.

If you require secure unit authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable secure unit authentication for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
user-authentication	Requires users behind a hardware client to identify themselves to the security appliance before connecting.

security-level

To set the security level of an interface, use the **security-level** command in interface configuration mode. To set the security level to the default, use the **no** form of this command. The security level protects higher security networks from lower security networks by imposing additional protection between the two.

security-level *number*

no security-level

Syntax Description

number	An integer between 0 (lowest) and 100 (highest).

Defaults

By default, the security level is 0.

If you name an interface “inside” and you do not set the security level explicitly, then the security appliance sets the security level to 100 (see the **nameif** command). You can change this level if desired.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **nameif** command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

  For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  For same security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

  Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

  For same security interfaces, you can configure **established** commands for both directions.

Normally, interfaces on the same security level cannot communicate. If you want interfaces on the same security level to communicate, see the **same-security-traffic** command. You might want to assign two interfaces to the same level and allow them to communicate if you want to create more than 101 communicating interfaces, or you want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Examples

The following example configures the security levels for two interfaces to be 100 and 0:

```
hostname(config)# interface gigabitethernet0/0
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear local-host	Resets all connections.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
vlan	Assigns a VLAN ID to a subinterface.

send response

To send a RADIUS Accounting-Response Start and Accounting-Response Stop message to the sender of the RADIUS Accounting-Request Start and Stop messages, use the **send response** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

send response

no send response

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to send a response with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

seq-past-window

To set the action for packets that have past-window sequence numbers (the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window), use the **seq-past-window** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

seq-past-window {**allow** | **drop**}

no seq-past-window

Syntax Description

allow	Allows packets that have past-window sequence numbers. This action is only allowed if the **queue-limit** command is set to 0 (disabled).
drop	Drops packets that have past-window sequence numbers.

Defaults

The default action is to drop packets that have past-window sequence numbers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **seq-past-window**—In tcp-map configuration mode, you can enter the **seq-past-window** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the security appliance to allow packets that have past-window sequence numbers:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# seq-past-window allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
queue-limit	Sets the out-of-order packet limit.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

serial-number

To include the security appliance serial number in the certificate during enrollment, use the **serial-number** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

serial-number

no serial-number

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to not include the serial number.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the security appliance serial number in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

server

To specify a default e-mail proxy server, use the **server** command in the applicable e-mail proxy mode. To remove the attribute from the configuration, use the **no** version of this command. The security appliance sends requests to the default e-mail server when the user connects to the e-mail proxy without specifying a server. If you do not configure a default server, and a user does not specify a server, the security appliance returns an error.

server {*ipaddr or hostname***}**

no server

Syntax Description

hostname	The DNS name of the default e-mail proxy server.
ipaddr	The IP address of the default e-mail proxy server.

Defaults

There is no default e-mail proxy server by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set a default POP3S e-mail server with an IP address. of 10.1.1.7:

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server (tls-proxy)

To specify the proxy trustpoint certificate presented during TLS handshake, use the **server** command in TLS proxy configuration mode. To remove the configuration, use the **no** form of this command.

server trust-point *p_tp*

no server trust-point *p_tp*

Syntax Description

trust-point *p_tp*	Specifies the defined trustpoint.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
TLS proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **server** command in TLS proxy configuration mode to control the TLS handshake parameters for the security appliance as the TLS server role in TLS proxy. It specifies the proxy trustpoint certificate presented during TLS handshake. This value corresponds to the trustpoint defined by the **crypto ca trustpoint** command. It can be self-signed or enrolled with a certificate authority.

The **server** command takes precedence over the global **ssl trust-point** command.

Examples

The following example shows how to create a TLS proxy instance:

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
client	Sets the TLS handshake parameters for the security appliance as the TLS client role in TLS proxy.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

server authenticate-client

To enable the security appliance to authenticate the TLS client during TLS handshake, use the **server authenticate-client** command in tls-proxy configuration mode.

To bypass client authenticaion, use the **no** form of this command.

server authenticate-client

no server authenticate-client

Syntax Description

There are no keywords or arguments for this command.

Defaults

This command is enabled by default, which means the TLS client is required to present a certificate during handshake with the security appliance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
TLS-proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Use the **server authenticate-client** command to control whether a client authentication is required during TLS Proxy handshake. When enabled (by default), the security appliance sends a Certificate Request TLS handshake message to the TLS client, and the TLS client is required to present its certificate.

Use the **no** form of this command to disable client authentication. Disabling TLS client authentication is suitable when the security appliance must interoperate with CUMA client or clients such as a Web browser that are incapable of sending a client certificate.

Examples

The following example configures a TLS proxy instance with client authentication disabled:

```
hostname(config)# tls-proxy mmp_tls
hostname(config-tlsp)# no server authenticate-client
hostname(config-tlsp)# server trust-point cuma_server_proxy
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.

server-port

To configure a AAA server port for a host, use the **server-port** command in aaa-server host mode. To remove the designated server port, use the **no** form of this command:

server-port *port-number*

no server-port

Syntax Description

port-number	A port number in the range 0 through 65535.

Defaults

The default server ports are as follows:

- SDI—5500
- LDAP—389
- Kerberos—88
- NT—139
- TACACS+—49

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server group	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example configures an SDI AAA server named “srvgrp1” to use server port number 8888:

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
```

Related Commands

Command	Description
aaa-server host	Configures host-specific AAA server parameters.

clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

server-separator

To specify a character as a delimiter between the e-mail and VPN server names, use **server-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the no form of this command.

server-separator {*symbol***}**

no server-separator

Syntax Description

symbol	The character that separates the e-mail and VPN server names. Choices are "@," (at) "|" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Defaults

The default is "@" (at).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The server separator must be different from the name separator.

Examples

The following example shows how to set a pipe (|) as the server separator for IMAP4S:

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

Related Commands

Command	Description
name-separator	Separates the e-mail and VPN usernames and passwords.

server-type

To manually configure the LDAP server model, use the **server-type** command in aaa-server host configuration mode. The security appliance supports the following server models:

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server, formerly named the Sun ONE Directory Server
- Generic LDAP directory servers that comply with LDAPv3 (no password management)

To disable this command, use the **no** form of this command.

server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

no server-type {**auto-detect | microsoft** | **sun** | **generic | openldap | novell**}

Syntax Description

auto-detect	Specifies that the security appliance determines the LDAP server type through auto-detection.
generic	Specifies LDAP v3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers.
microsoft	Specifies that the LDAP server is a Microsoft Active Directory.
openldap	Specifies that the LDAP server is an OpenLDAP server.
novell	Specifies that the LDAP server is a Novell server.
sun	Specifies that the LDAP server is a Sun Microsystems JAVA System Directory Server.

Defaults

By default, auto-detection attempts to determine the server type.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(2)	Support for the OpenLDAP and Novell server types was added.

Usage Guidelines

The security appliance supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server, the Microsoft Active Directory, and other LDAPv3 directory servers.

Note

- Sun—The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—Password management features are not supported.

By default, the security appliance auto-detects whether it is connected to a Microsoft directory server, a Sun LDAP directory server, or a generic LDAPv3 server. However, if auto-detection fails to determine the LDAP server type and if you know the server is either a Microsoft or Sun server, you can use the **server-type** command to manually configure the server as either a Microsoft or a Sun Microsystems LDAP server.

Examples

The following example, entered in aaa-server host configuration mode, configures the server type for the LDAP server ldapsvr1 at IP address 10.10.0.1. The first example configures a Sun Microsystems LDAP server.

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
```

The following example specifies that the security appliance use auto-detection to determine the server type:

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
sasl-mechanism	Configures SASL authentication between the LDAP client and server.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

server trust-point

To specify the proxy trustpoint certificate to present during TLS handshake, use the **server trust-point** command in TLS server configuration mode.

server trust-point *proxy_trustpoint*

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
TLS-proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The trustpoint can be self-signed, enrolled with a certificate authority, or from an imported credential. The **server trust-point** command has precedence over the global **ssl trust-point** command.

The **server trust-point** command specifies the proxy trustpoint certificate presented during TLS handshake. The certificate must be owned by the security appliance (identity certificate). The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential.

Create TLS proxy instances for each entity that can initiate a connection. The entity that initiates the TLS connection is in the role of TLS client. Because the TLS Proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Note When you are creating the TLS proxy instance to use with the Phone Proxy, the server trustpoint is the internal Phone Proxy trustpoint created the CTL file instance. The trustpoint name is in the form *internal_PP_<ctl-file_instance_name>*

Examples

The following example shows the use of the **server trust-point** command to specify the proxy trustpoint certificate to present during TLS handshake:

```
hostname(config-tlsp)# server trust-point ent_y_proxy
```

Related Commands

Command	Description
client (tls-proxy)	Configures trustpoints, keypairs, and cipher suites for a TLS proxy instance.
client trust-point	Specifies the proxy trustpoint certificate to present during TLS handshake.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.
tls-proxy	Configures a TLS proxy instance.

service

To enable resets for denied TCP connections, use the **service** command in global configuration mode. To disable resets, use the **no** form of this command.

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

Syntax Description

interface *interface_name*	Enables or disables resets for the specified interface.
resetinbound	Sends TCP resets for all inbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets. If you do not specify an interface, then this setting applies to all interfaces.
resetoutbound	Sends TCP resets for all outbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets. This option is enabled by default. You might want to disable outbound resets to reduce the CPU load during traffic storms, for example.
resetoutside	Enables resets for TCP packets that terminate at the least secure interface and are denied by the security appliance based on access lists or AAA settings. When this option is not enabled, the security appliance silently discards the packets of denied packets. We recommend that you use the **resetoutside** keyword with interface PAT. This keyword allows the security appliance to terminate the IDENT from an external SMTP or FTP server. Actively resetting these connections avoids the 30-second timeout delay.

Defaults

By default, **service resetoutbound** is enabled for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	The **interface** keyword and the **resetoutbound** command were added.

Usage Guidelines

You might want to explicitly send resets for inbound traffic if you need to reset identity request (IDENT) connections. When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance.

Examples

The following example disables outbound resets for all interfaces except for the inside interface:

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

The following example enables inbound resets for all interfaces except for the DMZ interface:

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

The following example enables resets for connections that terminate on the outside interface:

```
hostname(config)# service resetoutside
```

Related Commands

Command	Description
show running-config service	Displays the service configuration.

service (ctl-provider)

To specify the port to which the Certificate Trust List provider listens, use the **service** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

service port *listening_port*

no service port *listening_port*

Syntax Description

port *listening_port*	Specifies the certificate to be exported to the client.

Defaults

Default port is 2444.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **service** command in CTL provider configuration mode to specify the port to which the CTL provider listens. The port must be the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default port is 2444.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.

Commands	Description
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

service password-recovery

To enable password recovery, use the **service password-recovery** command in global configuration mode. To disable password recovery, use the **no** form of this command. Password recovery is enabled by default, but you might want to disable it to ensure that unauthorized users cannot use the password recovery mechanism to compromise the security appliance.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

Password recovery is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

On the ASA 5500 series adaptive security appliance, if you forget the passwords, you can boot the security appliance into ROMMON by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then set the security appliance to ignore the startup configuration by changing the configuration register (see the **config-register** command). For example if your configuration register is the default 0x1, then change the value to 0x41 by entering the **confreg 0x41** command. After reloading the security appliance, it loads a default configuration, and you can enter privileged EXEC mode using the default passwords. Then load the startup configuration by copying it to the running configuration and reset the passwords. Finally, set the security appliance to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the PIX 500 series security appliance, boot the security appliance into monitor mode by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then download the PIX password tool to the security appliance, which erases all passwords and **aaa authentication** commands.

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on using ROMMON and maintaining the

existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), then the security appliance changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Examples

The following example disables password recovery for the ASA 5500 series adaptive security appliance:

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

The following example disables password recovery for the PIX 500 series security appliance:

```
hostname(config)# no service password-recovery
WARNING: Saving "no service password-recovery" in the startup-config will disable password
recovery via the npdisk application.  The only means of recovering from lost or forgotten
passwords will be for npdisk to erase all file systems including configuration files and
images.  You should make a backup of your configuration and have a mechanism to restore
images from the Monitor Mode command line.
```

The following example for the ASA 5500 series adaptive security appliance shows when to enter ROMMON at startup and how to complete a password recovery operation.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...
```

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
config-register	Sets the security appliance to ignore the startup configuration when it reloads.
enable password	Sets the enable password.
password	Sets the login password.

service-policy (class)

To apply a hierarchical policy map under another policy map, use the **service-policy** command in class configuration mode. To disable the service policy, use the **no** form of this command. Hierarchical policies are supported only for QoS traffic shaping when you want to perform priority queueing on a subset of shaped traffic.

service-policy *policymap_name*

no service-policy *policymap_name*

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map that includes the **priority** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used (the **priority-queue** command).

For hierarchical priority-queueing, perform the following tasks using Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.

c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.

4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

Related Commands

Command	Description
class (policy-map)	Identifies a class map for a policy map.
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
policy-map	Identifies actions to perform on class maps.
priority	Enables priority queueing.
service-policy (global)	Applies a policy map to an interface.
shape	Enables traffic shaping.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

service-policy (global)

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in global configuration mode. To disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.

service-policy *policymap_name* [**global** | **interface** *intf*]

no service-policy *policymap_name* [**global** | **interface** *intf*]

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map, and not an inspection policy map (**policy-map type inspect**).
global	Applies the policy map to all interfaces.
interface *intf*	Applies the policy map to a specific interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To enable the service policy, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features*—For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more details about the commands available for each feature.
3. **service-policy**—Assigns the policy map to an interface or globally.

Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with inspections, and an interface policy with TCP normalization, then both inspections and TCP normalization are applied to the interface. However, if you have a global policy with inspections, and an interface policy with inspections, then only the interface policy inspections are applied to that interface.

By default, the configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.

The default service policy includes the following command:

```
service-policy global_policy global
```

Examples

The following example shows how to enable the inbound_policy policy map on the outside interface:

```
hostname(config)# service-policy inbound_policy interface outside
```

The following commands disable the default global policy, and enables a new one called new_global_policy on all other security appliance interfaces:

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
service-policy (class)	Applies a hierarchical policy under another policy map.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

session

To establish a Telnet session to an intelligent SSM, such as an AIP SSM or a CSC SSM, use the **session** command in privileged EXEC mode.

session *slot* [**do** | **ip**]

Syntax Description

do	Executes a command on the SSM specified by the *slot* argument. Do not use the **do** keyword unless you are advised to do so by Cisco TAC.
ip	Configures logging IP addresses for the SSM specified by the *slot* argument. Do not use the **ip** keyword unless you are advised to do so by Cisco TAC.
slot	Specifies the SSM slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **do** and **ip** keywords were added. These keywords are for use only when advised to do so by Cisco TAC.

Usage Guidelines

This command is only available when the SSM is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6** then the **X** key.

Examples

The following example sessions to an SSM in slot 1:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Related Commands

Command	Description
debug session-command	Shows debug messages for sessions.

set connection

To specify connection limits within a policy map for a traffic class, use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
random-sequence-number {enable | disable}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

Defaults

For the **conn-max**, **embryonic-conn-max**, **per-client-embryonic-max**, and **per-client-max** parameters, the default value of *n* is 0, which allows unlimited connections.

Sequence number randomization is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **per-client-embryonic-max** and **per-client-max** keywords were added.
8.0(2)	This command is now available for a Layer 3/4 management class map, for to-the-security appliance management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command (for through traffic) or **class-map type management** command (for management traffic). Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Note You can also configure maximum connections, maximum embryonic connections, and TCP sequence randomization in the NAT configuration. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

TCP Intercept Overview

Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the security appliance acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the security appliance receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

Disabling TCP Intercept for Management Packets for Clientless SSL Compatibility

By default, TCP management connections have TCP Intercept always enabled. When TCP Intercept is enabled, it intercepts the 3-way TCP connection establishment handshake packets and thus deprives the security appliance from processing the packets for clientless SSL. Clientless SSL requires the ability to

process the 3-way handshake packets to provide selective ACK and other TCP options for clientless SSL connections. To disable TCP Intercept for management traffic, you can set the embryonic connection limit; only after the embryonic connection limit is reached is TCP Intercept enabled.

TCP Sequence Randomization Overview

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predecting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.

Examples

The following is an example of the use of the **set connection** command configure the maximum number of simultaneous connections as 256 and to disable TCP sequence number randomization:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

The following is an example of the use of the **set connection** command in a service policy that diverts traffic to a CSC SSM. The **set connection** command restricts each client whose traffic the CSC SSM scans to a maximum of five connections.

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

You can enter this command with multiple parameters or you can enter each parameter as a separate command. The security appliance combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

the output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection conn-max 600 embryonic-conn-max 50
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.

clear configure policy-map	Removes all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy-map configurations.
show service-policy	Displays service policy configuration. Use the **set connection** keyword to view policies that include the **set connection** command.

set connection advanced-options

To specify advanced TCP connection options within a policy-map for a traffic class, use the **set connection advanced-options** command in class mode. To remove advanced TCP connection options for a traffic class within a policy map, use the **no** form of this command.

set connection advanced-options *tcp-mapname*

no set connection advanced-options *tcp-mapname*

Syntax Description

tcp-mapname	Name of a TCP map in which advanced TCP connection options are configured.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have configured the **policy-map** command and the **class** command, as well as the TCP map name, before issuing this command. See the description of the **tcp-map** command for detailed information.

Examples

The following example shows the use of the **set connection advanced-options** command to specify the use of a TCP map named localmap:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
class-map	Configures a traffic class by issuing at most one (with the exception of tunnel-group and default-inspection-traffic) match command, specifying match criteria, in the class-map mode.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

set connection decrement-ttl

To decrement the time to live value within a policy map for a traffic class, use the **set connection decrement-ttl** command in class configuration mode. To not decrement the time to live, use the **no** form of this command.

set connection decrement-ttl

no set connection decrement-ttl

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not decrement the time to live.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

This command, along with the **icmp unreachable** command, is required to allow a traceroute through the security appliance that shows the security appliance as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
clear configure policy-map	Removes all policy map configuration, except if a policy map is in use in a **service-policy** command, that policy map is not removed.

icmp unreachable	Controls the rate at which ICMP unreachables are allowed through the security appliance.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Displays service policy configuration.

set connection timeout

To specify connection timeouts within a policy map for a traffic class, use the **set connection timeout** command in class configuration mode. To remove the timeout, use the **no** form of this command.

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

Syntax Description

dcd	Enables dead connection detection (DCD). DCD detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist. After a TCP connection times out, the security appliance sends DCD probes to the end hosts to determine the validity of the connection. If one of the end hosts fails to respond after the maximum retries are exhausted, the security appliance frees the connection. If both end hosts respond that the connection is valid, the security appliance updates the activity timeout to the current time and reschedules the idle timeout accordingly.
embryonic *hh*:*mm*:*ss*	Sets the timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:0:0. The default is 0:0:30. You can also set the value to 0, which means the connection never times out. A TCP connection for which a three-way handshake is not complete is an embryonic connection.
half-closed *hh*:*mm*:*ss*	Sets the idle timeout period until a half-closed connection is closed, between 0:5:0 and 1193:0:0. The default is 0:10:0. You can also set the value to 0, which means the connection never times out. Half-closed connections are not affected by DCD. Also, the security appliance does not send a reset when taking down half-closed connections.
max_retries	Sets the number of consecutive failed retries for DCD before declaring the connection as dead. The minimum value is 1 and the maximum value is 255. The default is 5.
reset	Sends a reset to TCP endpoints when the connection times out. The security appliance sends the reset packet only in response to a host sending another packet for the timed-out flow (on the same source and destination port). The host then removes the connection from its connection table after receiving the reset packet. The host application can then attempt to establish a new connection using a SYN packet.
retry_interval	Time duration in *hh*:*mm*:*ss* format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15.
tcp *hh*:*mm*:*ss*	Sets the idle timeout period after which an established connection closes.

Defaults

The default **embryonic** timeout is 30 seconds.

The default **half-closed** idle timeout is 10 minutes.

The default **dcd** *max_retries* value is 5.

The default **dcd** *retry_interval* value is 15 seconds.

The default **tcp** idle timeout is 1 hour.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Support for DCD was added.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command. Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection timeout** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Enabling DCD changes the behavior of idle-timeout handling in the TCP normalizer. DCD probing resets the idle timeout on the connections seen in the **show conn** command. To determine when a connection that has exceeded the configured timeout value in the timeout command but is kept alive due to DCD probing, the **show service-policy** command includes counters to show the amount of activity from DCD.

Examples

The following example sets the connection timeouts for all traffic:

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection timeout tcp 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

You can enter **set connection** commands with multiple parameters or you can enter each parameter as a separate command. The security appliance combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection timeout embryonic 0:40:0
```

the output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configure connection values.
show running-config policy-map	Display all current policy-map configurations.
show service-policy	Displays counters for DCD and other service activity.

set metric

To set the metric value for a routing protocol, use the **set metric** command in route-map configuration mode. To return to the default metric value, use the **no** form of this command.

set metric *value*

no set metric *value*

Syntax Description

value	Metric value.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **no set metric** *value* command allows you to return to the default metric value. In this context, the *value* is an integer from 0 to 4294967295.

Examples

The following example shows how to configure a route map for OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

set metric-type

To specify the type of OSPF metric routes, use the **set metric-type** command in route-map configuration mode. To return to the default setting, use the **no** form of this command.

set metric-type {**type-1** | **type-2**}

no set metric-type

Syntax Description

type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.

Defaults

The default is **type-2**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to configure a route map for OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# set metric-type type-2
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

setup

To configure a minimal configuration for the security appliance using interactive prompts, enter the **setup** command in global configuration mode. This configuration provides connectivity to use ASDM. See also the **configure factory-default** command to restore the default configuration.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The setup dialog automatically appears at boot time if there is no startup configuration in Flash memory.

Before you can use the **setup** command, you must have an inside interface already configured. The PIX 500 series default configuration includes an inside interface (Ethernet 1), but the ASA 550 series default configuration does not. Before using the **setup** command, enter the **interface** command for the interface you want to make inside, and then the **nameif inside** command.

In multiple context mode, you can use the **setup** command in the system execution space and for each context.

When you enter the **setup** command, you are asked for the information in Table 24-1. The system **setup** command includes a subset of these prompts. If there is already a configuration for the prompted parameter, it appears in barckets so you can either accept it as the default or override it by entering something new.

Table 24-1 Setup Prompts

Prompt	Description
`Pre-configure Firewall now through interactive prompts [yes]?`	Enter **yes** or **no**. If you enter **yes**, the setup dialog continues. If **no**, the setup dialog stops and the global configuration prompt (`hostname(config)#`) appears.

Table 24-1 Setup Prompts (continued)

`Firewall Mode [Routed]:`	Enter **routed** or **transparent**.
`Enable password:`	Enter an enable password. (The password must have at least three characters.)
`Allow password recovery [yes]?`	Enter **yes** or **no**.
`Clock (UTC):`	You cannot enter anything in this field. UTC time is used by default.
`Year:`	Enter the year using four digits, for example, 2005. The year range is 1993 to 2035.
`Month:`	Enter the month using the first three characters of the month; for example, **Sep** for September.
`Day:`	Enter the day of the month, from 1 to 31.
`Time:`	Enter the hour, minutes, and seconds in 24-hour time format. For example, enter **20:54:44** for 8:54 p.m and 44 seconds.
`Inside IP address:`	Enter the IP address for the inside interface.
`Inside network mask:`	Enter the network mask that applies to the inside IP address. You must specify a valid network mask, such as 255.0.0.0 or 255.255.0.0.
`Host name:`	Enter the hostname that you want to display in the command line prompt.
`Domain name:`	Enter the domain name of the network on which the security appliance runs.
`IP address of host running Device Manager:`	Enter the IP address of the host that needs to access ASDM.
`Use this configuration and write to flash?`	Enter **yes** or **no**. If you enter **yes**, the inside interface is enabled and the requested configuration is written to the Flash partition. If you enter **no**, the setup dialog repeats, beginning with the first question: `Pre-configure Firewall now through interactive prompts [yes]?` Enter **no** to exit the setup dialog or **yes** to repeat it.

Examples

This example shows how to complete the **setup** command prompts:

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
```

```
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

Related Commands

Command	Description
configure factory-default	Restores the default configuration.

shape

To enable QoS traffic shaping, use the **shape** command in class configuration mode. If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate, called *traffic shaping*. To remove this configuration, use the **no** form of this command.

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

Syntax Description

average *rate*	Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000. See the "Usage Guidelines" section for more information about how the time period is calculated.
burst_size	Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Defaults

If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class configuration	•	•	•	—	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable traffic shaping, use the Modular Policy Framework:

1. **policy-map**—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.

b. **shape**—Apply traffic shaping to the class map.

c. (Optional) **service-policy**—Call a different policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.

2. **service-policy**—Assigns the policy map to an interface or globally.

Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPSec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the burst size value. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the token bucket.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queueing, see the **priority** command):
  - The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
  - When the queue limit is reached, packets are tail-dropped.
  - Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
  - The time interval is derived by *time_interval* = *burst_size* / *average_rate*. The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

    Average Rate = 1000000

    Burst Size = 1000000

    In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

How QoS Features Interact

You can configure each of the QoS features alone if desired for the security appliance. Often, though, you configure multiple QoS features on the security appliance so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).

  You cannot configure priority queueing and policing for the same set of traffic.
- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

You cannot configure traffic shaping and standard priority queueing for the same interface; only hierarchical priority queueing is allowed. For example, if you configure standard priority queueing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the security appliance does not restrict you from configuring this.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

Related Commands

Command	Description
class	Identifies the class map on which you want to perform actions in a policy map.
police	Enables QoS policing.
policy-map	Identifies actions to apply to traffic in a service policy.
priority	Enables QoS priority queueing.
service-policy (class)	Applies a hierarchical policy map.
service-policy (global)	Applies a service policy to interface(s).
show service-policy	Shows QoS statistics.

show aaa local user

To show the list of usernames that are currently locked, or to show details about the username, use the show **aaa local user** command in global configuration mode.

show aaa local user [**locked]**

Syntax Description

locked	(Optional) Shows the list of usernames that are currently locked.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you omit the optional keyword **locked**, the security appliance displays the failed-attempts and lockout status details for all AAA local users.

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Examples

The following example shows use of the **show aaa local user** command to display the lockout status of all usernames:

This example shows the use of the **show aaa local user** command to display the number of failed authentication attempts and lockout status details for all AAA local users, after the limit has been set to 5:

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

This example shows the use of the **show aaa local user** command with the **lockout** keyword to display the number of failed authentication attempts and lockout status details only for any locked-out AAA local users, after the limit has been set to 5:

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                  6       Y       test
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures the maximum number of times a user can enter a wrong password before being locked out.
clear aaa local user fail-attempts	Resets the number of failed attempts to 0 without modifying the lockout status.
clear aaa local user lockout	Clears th e lockout status of the specified user or all users and sets their failed attempts counters to 0.

show aaa-server

To display AAA server statistics for AAA servers, use the **show aaa-server** command in privileged EXEC mode.

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Shows statistics for the LOCAL user database.
groupname	(Optional) Shows statistics for servers in a group.
host *hostname*	(Optional) Shows statistics for a particular server in the group.
protocol *protocol*	(Optional) Shows statistics for servers of the specified protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

By default, all AAA server statistics display.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.1(1)	The http-form protocol was added.
8.0(2)	The server status now shows if the status was changed manually using the **aaa-server active** or **fail** command.

Examples

This example shows the use of the **show aaa-server** command to display statistics for a particular host in server group group1:

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
```

```
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

Field descriptions for the **show aaa-server** command are shown below:

Field	Description
Server Group	The server group name specified by the **aaa-server** command.
Server Protocol	The server protocol for the server group specified by the **aaa-server** command.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the security appliance and the AAA server. You can specify the RADIUS authentication port using the **authentication-port** command. You can specify the RADIUS accounting port using the **accounting-port** command. For non-RADIUS servers, the port is set by the **server-port** command.
Server status	The status of the server. You see one of the following values: • ACTIVE—The security appliance will communicate with this AAA server. • FAILED—The security appliance cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated. If the status is followed by "(admin initiated)," then the server was manually failed or reactivated using the **aaa-server active** or **fail** command. You also see the date and time of the last transaction in the following form: **Last transaction** ({**success** | **failure**}) **at** *time timezone date* If the security appliance has never communicated with the server, the message shows as the following: **Last transaction at Unknown**
Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.

Field	Description
Number of authentication requests	The number of authentication requests sent by the security appliance. This value does not include retransmissions after a timeout.
Number of authorization requests	The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic (for TACACS+ servers), or for WebVPN and IPSec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout
Number of accounting requests	The number of accounting requests. This value does not include retransmissions after a timeout
Number of retransmissions	The number of times a message was retransmitted after an internal timeout. This value applies only to Kerberos and RADIUS servers (UDP)
Number of accepts	The number of successful authentication requests.
Number of rejects	The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.
Number of challenges	The number of times the AAA server required additional information from the user after receiving the initial username and password information.
Number of malformed responses	N/A. Reserved for future use.
Number of bad authenticators	The number of times that one of the following occurs: • The “authenticator” string in the RADIUS packet is corrupted (rare). • The shared secret key on the security appliance does not match the one on the RADIUS server. To fix this problem, enter the proper server key. This value only applies to RADIUS.
Number of timeouts	The number of times the security appliance has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.
Number of unrecognized responses	The number of times that the security appliance received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server got corrupted, which is rare.

Related Commands

Command	Description
show running-config aaa-server	Display statistics for all servers in the indicated server group or for a particular server.
clear aaa-server statistics	Clear the AAA server statistics.

show access-list

To display the counters for an access list, use the **show access-list** command in privileged EXEC mode.

show access-list *id_1* [...[*id_2*]] [**brief**]

Syntax Description

acl_name_ 1	A name or set of characters that identifies an existing access list.
acl_name_2	A name or set of characters that identifies an existing access list.
brief	Displays the access list identifiers and hit count in hexadecimal format.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	Support for the **brief** keyword was introduced.

Usage Guidelines

You can display multiple access lists at one time by entering the access list identifiers in one command.

You can specify the **brief** keyword to display access list hit count and identifiers information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in two columns, and are the same identifiers used in syslog 106023 and 106100.

Examples

The following is sample output from the **show access-list** command:

```
hostname# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 10 elements
access-list 101 line 1 extended permit tcp any eq www any (hitcnt=0) 0xa14fc533
access-list 101 line 2 extended permit tcp any eq www any eq www (hitcnt=0) 0xaa73834e
access-list 101 line 3 extended permit tcp any eq www any range telnet www (hitcnt=0)
0x49ac02e6
access-list 101 line 4 extended permit tcp any range telnet www any range telnet www
(hitcnt=0) 0xa0021a9f
access-list 101 line 5 extended permit udp any range biff www any (hitcnt=0) 0xf89a7328
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43 access-list
101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
```

```
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

The output contains a unique hexamdecimal identifier for each access control entry at the end of each line.

The following is sample output from the **show access-list brief** command:

```
hostname (config)# sh access-list abc brief

abc:
28676dfa 00000000 00000001
bbec063f f0109e02 000000a1
3afd0576 f0109e02 000000c2
a83ddc02 f0109e02 00000021
hostname (config)#
```

The first two columns display identifiers in hexadecimal format, and the third column lists the hit count in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. If the hit count is zero, no information is displayed.

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show running-config access-list	Displays the current running access-list configuration.

show activation-key

To display the running activation key and licensed features in the configuration that are enabled by your activation key, including the number of contexts allowed, use the **show activation-key** command in privileged EXEC mode.

show activation-key [detail]

Note This command is not supported on the PIX platform.

Syntax Description

The **detail** keyword displays the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	The **detail** keyword was added.

Usage Guidelines

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the security appliance flash file system is the same as the activation key running on the security appliance, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the security appliance flash file system is different from the activation key running on the security appliance, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If you downgrade your activation key, the display shows that the running key (the old key) differs from the key that is stored in the Flash (the new key). When you restart, the security appliance uses the new key.

- If you upgrade your key to enable extra features, the new key starts running immediately without a restart.
- For the PIX Firewall platform, if there is any change in the failover feature (R/UR/FO) between the new key and the old key, it prompts for confirmation. If the user enters **n**, it aborts the change; otherwise it updates the key in the Flash file system. When you restart the security appliance uses the new key.
- If you downgrade to an earlier release, your key for the current release might allow for more security contexts than the earlier release supports. When the value of the security contexts in the key exceeds the platform limit, the following message appears in the show activation-key output:

  ```
  The Running Activation Key feature: 50 security contexts exceeds the limit in the
  platform, reduce to 20 security contexts.
  ```

- If you downgrade to an earlier release, your key for the current release might enable GTP/GPRS even though it is not allowed in the earlier release. When the key enables GTP/GPRS but the software version does not allow it, the following message appears in the show activation-key output:

  ```
  The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
  GTP/GPRS.
  ```

A temporary activation key is a time-based activation key, which you activate or deactivate using the **activation-key** command. When you deactivate a temporary activation key, you may assign a permanent activation key. A permanent activation key is a nontime-based activation key. You cannot delete temporary activation keys, because you can reactivate them at a later date.

Both temporary and permanent activation keys are stored on the flash file system. The running activation key is the one being applied. You may apply only one temporary activation key at a time. If you apply a temporary activation key on a security appliance that already has a temporary activation key, the old temporary activation key is deactivated and the new temporary activation key is applied.

The security appliance tracks all temporary activation keys that have been activated. When a temporary activation key expires, the security appliance notifies you of the expiration. After the temporary activation key expires, it can no longer appear. Non-active temporary activation keys are keys that have been applied and then overwritten by another temporary or permanent activation key.

Examples

This example shows how to display the commands in the configuration for features that are enabled by your activation key:

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada
The Running Activation Key feature: 50 security contexts exceeds the limit in the
platform, reduce to 20 security contexts.
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
GTP/GPRS.

License Features for this Platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 50
Inside Hosts                : Unlimited
Failover                    : Enabled
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL-filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
```

```
VPN Peers                    : 5000
Advanced Endpoint Assessment: Disabled
UC Proxy Sessions            : 2

The flash activation key is the SAME as the running key.
```

This example shows how to display the licensed features in the configuration that are enabled by temporary and permanent activation keys:

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
Permanent Flash Activation Key: 0x31245147 0x3834b49a 0x98b391b4
0x95b83030 0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

Temporary Flash Activation Key: 0x051e96ff 0x98937617 0x79cbe717
0x502449e7 0x862b92ab

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Disabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
WebVPN Peers                 : 2
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions            : 2
This is a time-based license that will expire in 27 day(s).
```

This example shows how to display the licensed features in the configuration that are enabled by a permanent activation key:

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
No active temporary key.
Running Activation Key: 0x31245147 0x3834b49a 0x98b391b4 0x95b83030
0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
```

```
VPN-DES                       : Enabled
VPN-3DES-AES                  : Enabled
Security Contexts             : 50
GTP/GPRS                      : Enabled
VPN Peers                     : 5000
WebVPN Peers                  : 5000
AnyConnect for Mobile         : Enabled
AnyConnect for Linksys phone  : Enabled
Advanced Endpoint Assessment  : Enabled
UC Proxy Sessions             : 2

This platform has an ASA 5540 VPN Premium license.

The flash activation key is the SAME as the running key.

Non-active temporary keys:                                Time left
-----------------------------------------------------------------------
0x2a53d6   0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2  28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397  27 day(s
```

Related Commands

Command	Description
activation-key	Changes the activation key.

show ad-groups

To display groups that are listed on an Active Directory server, use the **show ad-groups** command in privileged EXEC mode:

show ad-groups *name* [**filter** *string*]

Syntax Description

name	The name of the Active Directory server group to query.
string	A string within quotes specifying all or part of the group name to search for.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **show ad-groups** command applies only to Active Directory servers that use the LDAP protocol to retrieve groups. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

When the LDAP attribute type = LDAP, the default time that the security appliance waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.

Note If the Active Directory server has a large number of groups, the output of the **show ad-groups** command may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

Examples

```
hostname# show ad-groups LDAP-AD17
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

The next example shows the same command with the **filter** option:

```
hostname(config)# show ad-groups LDAP-AD17 filter "Eng"
.
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
group-search-timeout	Adjusts the time the security appliance waits for a response from an Active Directory server for a list of groups.

show admin-context

To display the context name currently assigned as the admin context, use the **show admin-context** command in privileged EXEC mode.

show admin-context

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show admin-context** command. The following example shows the admin context called “admin” and stored in the root directory of flash:

```
hostname# show admin-context
Admin: admin flash:/admin.cfg
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
clear configure context	Removes all contexts.
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

show arp

To view the ARP table, use the **show arp** command in privileged EXEC mode.

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	Added dynamic ARP age to the display.

Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.”

Examples

The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
hostname# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp-inspection

To view the ARP inspection setting for each interface, use the **show arp-inspection** command in privileged EXEC mode.

show arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show arp-inspection** command:

```
hostname# show arp-inspection
interface               arp-inspection         miss
-----------------------------------------------------
inside1                 enabled                flood
outside                 disabled                -
```

The **miss** column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp statistics

To view ARP statistics, use the show arp statistics command in privileged EXEC mode.

show arp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show arp statistics** command:

```
hostname# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

Table 2 shows each field description.

Table 24-2 show arp statistics Fields

Field	Description
Number of ARP entries	The total number of ARP table entries.
Dropped blocks in ARP	The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.
Maximum queued blocks	The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.

Table 24-2 show arp statistics Fields (continued)

Field	Description
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all security appliance interfaces that were from the same IP address as that of a security appliance interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the security appliance as part of the ARP-Defense mechanism.
Total ARP retries	The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.
Unresolved hosts	The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.
Maximum unresolved hosts	The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the security appliance booted up.

Related Commands

Command	Description
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics and resets the values to zero.
show arp	Shows the ARP table.
show running-config arp	Shows the current configuration of the ARP timeout.

show asdm history

To display the contents of the ASDM history buffer, use the **show asdm history** command in privileged EXEC mode.

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

Syntax Description

asdmclient	(Optional) Displays the ASDM history data formatted for the ASDM client.
feature *feature*	(Optional) Limits the history display to the specified feature. The following are valid values for the *feature* argument: • **all**—Displays the history for all features (default). • **blocks**—Displays the history for the system buffers. • **cpu**—Displays the history for CPU usage. • **failover**—Displays the history for failover. • **ids**—Displays the history for IDS. • **interface** *if_name*—Displays the history for the specified interface. The *if_name* argument is the name of the interface as specified by the **nameif** command. • **memory**—Displays memory usage history. • **perfmon**—Displays performance history. • **sas**—Displays the history for Security Associations. • **tunnels**—Displays the history for tunnels. • **xlates**—Displays translation slot history.
snapshot	(Optional) Displays only the last ASDM history data point.
view *timeframe*	(Optional) Limits the history display to the specified time period. Valid values for the *timeframe* argument are: • **all**—all contents in the history buffer (default). • **12h**—12 hours • **5d**—5 days • **60m**—60 minutes • **10m**—10 minutes

Defaults

If no arguments or keywords are specified, all history information for all features is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm history** command to the **show asdm history** command.

Usage Guidelines

The **show asdm history** command displays the contents of the ASDM history buffer. Before you can view ASDM history information, you must enable ASDM history tracking using the **asdm history enable** command.

Examples

The following is sample output from the **show asdm history** command. It limits the output to data for the outside interface collected during the last 10 minutes.

```
hostname# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
```

```
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

The following is sample output from the **show asdm history** command. Like the previous example, it limits the output to data for the outside interface collected during the last 10 minutes. However, in this example the output is formatted for the ASDM client.

```
hostname# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|6
2469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|6
2553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|6
2636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|6
2723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|2
5026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|2
5102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|2
5169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|2
5381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750
|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|751|751|7
51|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753
|753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|5
5|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|5
5|55|55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|4
381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|5
401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698
|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349
|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|33
49|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|5
|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|7|
6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
```

```
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|3750
10|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|375
395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|37
5794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|3
76200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|1
28|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
hostname#
```

The following is sample output from the **show asdm history** command using the **snapshot** keyword:

```
hostname# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
```

```
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
```

```
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
```

```
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
hostname#
```

Related Commands

Command	Description
asdm history enable	Enables ASDM history tracking.

show asdm image

To the current ASDM software image file, use the show **asdm image** command in privileged EXEC mode.

show asdm image

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm image** command to the **show asdm image** command.

Examples

The following is sample output from the **show asdm image** command:

```
hostname# show asdm image

Device Manager image file, flash:/ASDM
```

Related Commands

Command	Description
asdm image	Specifies the current ASDM image file.

show asdm log_sessions

To display a list of active ASDM logging sessions and their associated session IDs, use the **show asdm log_sessions** command in privileged EXEC mode.

show asdm log_sessions

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the security appliance. Each ASDM logging session is assigned a unique session ID. You can use this session ID with the **asdm disconnect log_session** command to terminate the specified session.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

Examples

The following is sample output from the **show asdm log_sessions** command:

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect log_session	Terminates an active ASDM logging session.

show asdm sessions

To display a list of active ASDM sessions and their associated session IDs, use the **show asdm sessions** command in privileged EXEC mode.

show asdm sessions

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm sessions** command to the **show asdm sessions** command.

Usage Guidelines

Each active ASDM session is assigned a unique session ID. You can use this session ID with the **asdm disconnect** command to terminate the specified session.

Examples

The following is sample output from the **show asdm sessions** command:

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect	Terminates an active ASDM session.

CHAPTER 25

show asp drop through show curpriv Commands

show asp drop

To debug the accelerated security path dropped packets or connections, use the **show asp drop** command in privileged EXEC mode.

show asp drop [**flow [***flow_drop_reason***]** | **frame [***frame_drop_reason*]]

Syntax Description

flow [*flow_drop_reason*]	(Optional) Shows the dropped flows (connections). You can specify a particular reason by using the *flow_drop_reason* argument. Valid values for the *flow_drop_reason* argument are listed in the "Usage Guidelines" section, below.
frame [*frame_drop_reason*]	(Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Valid values for the *frame_drop_reason* argument are listed in the "Usage Guidelines" section, below.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Additional drop reasons were added.
7.2(1)	Additional drop reasons were added.
7.2(4)	Added a timestamp indicating when the last time the asp drop counters were cleared. It also displays the capture asp-drop type keywords next to the descriptions it displays.
8.0(2)	Additional drop reasons were added.
7.0(8)/7.2(4)/8.0(4)	Output now includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command using the keyword.

Usage Guidelines

The **show asp drop** command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Table 25-1 lists valid values for the *frame_drop_reason* argument for dropped frames. Table 25-2 lists valid values for the *flow_drop_reason* argument for dropped flows.

Table 25-1 Frame Drop Reasons

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
acl-drop	Flow is denied by access rule	This counter is incremented when a packet is denied by the security appliance. The deny rule could be a default rule created when the security appliance comes up, when various features are turned on or off, when an access list is applied to an interface, or any other feature. Apart from default rule drops, a flow could be denied because of: • An access list configured on an interface • An access list configured for AAA, and AAA denied the user • Through traffic arriving at a management-only interface • Unencrypted traffic arriving on a IPSec-enabled interface **Recommendation**: Check the access lists referenced by the following system log messages. **System log messages**: 106023, 106100, 106004
bad-crypto	Bad crypto return in packet	This counter will increment when the security appliance attempts to perform a crypto operation on a packet, and the crypto operation fails. This is not a normal condition and could indicate possible software or hardware problems with the security appliance. **Recommendation**: If you are receiving many bad crypto indications, your security appliance may need servicing. You should enable system message 402123 to determine whether the crypto errors are hardware or software errors. You can also check the error counter in the global IPSec statistics with the **show ipsec stats** command. If the IPSec SA that is triggering these errors is known, the SA statistics from the **show ipsec sa detail** command will also be useful in diagnosing the problem. **System log messages**: 402123

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
bad-ipsec-natt	Bad IPSEC NATT packet	This counter will increment when the security appliance receives a packet on an IPSec connection that has negotiated NAT-T, but the packet is not addressed to the NAT-T UDP destination port of 4500 or had an invalid payload length. **Recommendation**: Analyze your network traffic to determine the source of the NAT-T traffic. **System log messages**: None.
bad-ipsec-prot	IPSEC not AH or ESP	This counter will increment when the security appliance receives a packet on an IPSec connection that is not an AH or ESP protocol packet. This is not a normal condition. **Recommendation**: If you are receiving many IPSec not AH or ESP indications on your security appliance, analyze your network traffic to determine the source of the traffic. **System log messages**: 402115
bad-ipsec-udp	Bad IPSEC UDP packet	This counter will increment when the security appliance receives a packet on an IPSec connection that has negotiated IPSec over UDP, but the packet has an invalid payload length. **Recommendation**: Analyze your network traffic to determine the source of the NAT-T traffic. **System log messages**: None.
bad-tcp-cksum	Bad TCP checksum	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets, and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. To allow packets with an incorrect TCP checksum, disable the **checksum-verification** feature. **System log messages**: None
bad-tcp-flags	Bad TCP flags	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with invalid TCP flags in the TCP header. For example, a packet with both SYN and FIN TCP flags set will be dropped. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
conn-limit	Connection limit reached	This reason is given for dropping a packet when the connection limit or host connection limit has been exceeded. If this is a TCP packet which is dropped during TCP connection establishment phase due to connection limit, the drop reason "TCP connection limit reached" is also reported. **Recommendation**: If this is incrementing rapidly, check the System log messages to determine which host's connection limit is reached. The connection limit may need to be increased if the traffic is normal, or the host may be under attack. **System log messages**: 201011
ctm-error	CTM returned error	This counter will increment when the security appliance attempts to perform a crypto operation on a packet and the crypto operation fails. This is not a normal condition and could indicate possible software or hardware problems with the security appliance. **Recommendation**: If you are receiving many bad crypto indications, your security appliance may need servicing. You should enable system message 402123 to determine whether the crypto errors are hardware or software errors. You can also check the error counter in the global IPSec statistics with the **show ipsec stats** command. If the IPSec SA that is triggering these errors is known, the SA statistics from the **show ipsec sa detail** command will also be useful in diagnosing the problem. **System log messages**: 402123
dns-guard-id-not-matched	DNS Guard id not matched	This counter will increment when the identification of the DNS response message does not match any DNS queries that passed across the appliance earlier on the same connection. This counter will increment by the DNS Guard function. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: None.
dns-guard-out-of-app-id	DNS Guard out of app id	This counter will increment when the DNS Guard function fails to allocate a data structure to store the identification of the DNS message. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
dst-l2_lookup-fail	Dst MAC L2 Lookup Failed	This counter will increment when the security appliance is configured for transparent mode, and the security appliance does a Layer 2 destination MAC address lookup that fails. Upon the lookup failure, the security appliance will begin the destination MAC discovery process and attempt to find the location of the host via ARP and/or ICMP messages. **Recommendation**: This is a normal condition when the security appliance is configured for transparent mode. You can also execute the **show mac-address-table** command to list the L2 MAC address locations currently discovered by the security appliance. **System log messages**: None.
flow-expired	Expired flow	This counter is incremented when the security appliance tries to inject a new or cached packet belonging to a flow that has already expired. It is also incremented when the security appliance attempts to send an RST on a TCP flow that has already expired, or when a packet returns from the AIP SSM but the flow had already expired. The packet is dropped. **Recommendation**: If valid applications are getting preempted, investigate if a longer timeout is needed. **System log messages**: None.
fo-standby	Dropped by standby unit	If a through-the-box packet arrives at security appliance or context in a standby state, and a flow is created, then the packet is dropped and the flow removed. This counter will increment each time a packet is dropped in this manner. **Recommendation**: This counter should never be incrementing on the active security appliance or context. However, it is normal to see it increment on the standby appliance or security appliance. **System log messages**: 302014, 302016, 302018
fragment-reassembly-failed	Fragment reassembly failed	This counter is incremented when the security appliance fails to reassemble a chain of fragmented packets into a single packet. All the fragment packets in the chain are dropped. This is probably because of a failure while allocating memory for the reassembled packet. **Recommendation**: Use the **show blocks** command to monitor the current block memory. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
host-move-pkt	FP host move packet	This counter will increment when the security appliance or context is configured for transparent mode, and the source interface of a known Layer 2 MAC address is detected on a different interface. **Recommendation**: This indicates that a host has been moved from one interface (i.e. LAN segment) to another. This condition is normal while in transparent mode if the host has in fact been moved. However, if the host move toggles back and forth between interfaces, a network loop may be present. **System log messages**: 412001, 412002, 322001
ifc-classify	Virtual firewall classification failed	A packet arrived on a shared interface, but failed to classify to any specific context interface. **Recommendation**: Use the **global** or **static** command to specify the IPv4 addresses that belong to each context interface. **System log messages**: None.
inspect-dns-id-not-matched	DNS Inspect id not matched	This counter will increment when the identification of the DNS response message does not match any DNS queries that passed across the security appliance earlier on the same connection. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: None.
inspect-dns-invalid-domain-label	DNS Inspect invalid domain label	This counter will increment when the security appliance detects an invalid DNS domain name or label. DNS domain name and label is checked per RFC 1035. **Recommendation**: None. **System log messages**: None.
inspect-dns-invalid-pak	DNS Inspect invalid packet	This counter will increment when the security appliance detects an invalid DNS packet. For example, a DNS packet with no DNS header, the number of DNS resource records not matching the counter in the header, etc. **Recommendation**: None. **System log messages**: None.
inspect-dns-out-of-app-id	DNS Inspect out of app id	This counter will increment when the DNS inspection engine fails to allocate a data structure to store the identification of the DNS message. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
inspect-dns-pak-too-long	DNS Inspect packet too long	This counter is incremented when the length of the DNS message exceeds the configured maximum allowed value. **Recommendation**: No action required. If DNS message length checking is not desired, enable DNS inspection without the **inspect dns maximum-length** option. **System log messages**: 410001
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect different embedded conn	This counter will increment when the frame embedded in the ICMP error message does not match the established connection that has been identified when the ICMP connection is created. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: 313005
inspect-icmp-error-no-existing-conn	ICMP Error Inspect no existing conn	This counter will increment when the security appliance is not able to find any established connection related to the frame embedded in the ICMP error message. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: 313005
inspect-icmp-out-of-app-id	ICMP Inspect out of app id	This counter will increment when the ICMP inspection engine fails to allocate an App ID data structure. The structure is used to store the sequence number of the ICMP packet. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System log messages**: None.
inspect-icmp-seq-num-not-matched	ICMP Inspect seq num not matched	This counter will increment when the sequence number in the ICMP echo reply message does not match any ICMP echo message that passed across the security appliance earlier on the same connection. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: 313004

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect invalid packet	This counter will increment when the security appliance detects an invalid frame embedded in the ICMPv6 packet. This check is the same as that on IPv6 packets. For example, an incomplete IPv6 header, a malformed IPv6 Next Header, etc. **Recommendation**: None. **System log messages**: None.
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect no existing conn	This counter will increment when the security appliance is not able to find any established connection related to the frame embedded in the ICMPv6 error message. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System log messages**: 313005
inspect-rtcp-invalid-length	Invalid RTCP Packet length	This counter will increment when the UDP packet length is less than the size of the RTCP header. **Recommendation**: No action required. A capture can be used to figure out which RTP source is sending the incorrect packets and you can deny the host using the access lists. **System log messages**: None.
inspect-rtcp-invalid-payload-type	Invalid RTCP Payload type field	This counter will increment when the RTCP payload type field does not contain the values 200 to 204. **Recommendation**: The RTP source should be validated to see why it is sending payload types outside of the range recommended by the RFC 1889. **System log messages**: 431002
inspect-rtcp-invalid-version	Invalid RTCP Version field	This counter will increment when the RTCP version field contains a version other than 2. **Recommendation**: The RTP source in your network does not seem to be sending RTCP packets conformant with the RFC 1889. The reason for this has to be identified and you can deny the host using access lists if required. **System log messages**: 431002.
inspect-rtp-invalid-length	Invalid RTP Packet length	This counter will increment when the UDP packet length is less than the size of the RTP header. **Recommendation**: No action required. A capture can be used to figure out which RTP source is sending the incorrect packets and you can deny the host using the access lists. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
inspect-rtp-invalid-payload-type	Invalid RTP Payload type field	This counter will increment when the RTP payload type field does not contain an audio payload type when the signalling channel negotiated an audio media type for this RTP secondary connection. The counter increments similarly for the video payload type. **Recommendation**: The RTP source in your network is using the audio RTP secondary connection to send video or vice versa. If you wish to prevent this you can deny the host using access lists. **System log messages**: 431001
inspect-rtp-invalid-version	Invalid RTP Version field	This counter will increment when the RTP version field contains a version other than 2. **Recommendation**: The RTP source in your network does not seem to be sending RTP packets conformant with the RFC 1889. The reason for this has to be identified and you can deny the host using access lists if required. **System log messages**: 431001
inspect-rtp-max-outofseq-paks-probation	RTP out of sequence packets in probation period	This counter will increment when the out of sequence packets when the RTP source is being validated exceeds 20. During the probation period, the inspect looks for 5 in-sequence packets to consider the source validated. **Recommendation**: Check the RTP source to see why the first few packets do not come in sequence and correct it. **System log messages**: 431001
inspect-rtp-sequence-num-outofrange	RTP Sequence number out of range	This counter will increment when the RTP sequence number in the packet is not in the range expected by the inspect. **Recommendation**: No action is required because the inspect tries to recover and start tracking from a new sequence number after a lapse in the sequence numbers from the RTP source. **System log messages**: 431001
inspect-rtp-ssrc-mismatch	Invalid RTP Synchronization Source field	This counter will increment when the RTP SSRC field in the packet does not match the SSRC which the inspect has been seeing from this RTP source in all the RTP packets. **Recommendation**: This could be because the RTP source in your network is rebooting and hence changing the SSRC or it could be because of another host on your network trying to use the opened secondary RTP connections on the firewall to send RTP packets. This should be investigated further to confirm if there is a problem. **System log messages**: 431001

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
intercept-unexpected	Intercept unexpected packet	The security appliance either received data from a client while waiting for a SYNACK from a server, or it received a packet that cannot be handled in a particular state of TCP intercept. **Recommendation**: If this drop is causing the connection to fail, please have a sniffer trace of the client- and server-side of the connection while reporting the issue. The security appliance could be under attack, and the sniffer traces or capture would help narrow down the culprit. **System log messages**: None.
interface-down	Interface is down	This counter will increment for each packet received on an interface that is shutdown using the **shutdown** command. For ingress traffic, the packet is dropped after security context classification and if the interface associated with the context is shut down. For egress traffic, the packet is dropped when the egress interface is shut down. **Recommendation**: None. **System log messages**: None.
invalid-app-length	Invalid app length	This counter will increment when the security appliance detects an invalid length of the Layer 7 payload in the packet. Currently, it counts the drops by the DNS Guard function only. For example, an incomplete DNS header. **Recommendation**: None. **System log messages**: None.
invalid-encap	Invalid encapsulation	This counter is incremented when the security appliance receives a frame belonging to an unsupported link-level protocol or if the L3 type specified in the frame is not supported by the security appliance. The packet is dropped. **Recommendation**: Verify that directly-connected hosts have proper link-level protocol settings. **System log messages**: None.
invalid-ethertype	Invalid ethertype	This counter is incremented when the fragmentation module on the security appliance receives or tries to send a fragmented packet that does not belong to IP version 4 or version 6. The packet is dropped. **Recommendation**: Verify the MTU of the security appliance and other devices on the connected network to determine why the security appliance is processing such fragments. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
invalid-ip-header	Invalid IP header	This counter is incremented and the packet is dropped when the security appliance receives an IP packet whose computed checksum of the IP header does not match the recorded checksum in the header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a peer is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None
invalid-ip-length	Invalid IP length	This counter is incremented when the security appliance receives an IPv4 or IPv6 packet in which the header length or total length fields in the IP header are not valid or do not conform to the received packet length. **Recommendation**: None. **System log messages**: None.
invalid-ip-option	IP option configured drop	This counter is incremented when any unicast packet with IP options or a multicast packet with IP options that have not been configured to be accepted, is received by the security appliance. The packet is dropped. **Recommendation**: Investigate why a packet with IP options is being sent by the sender. **System log messages**: None.
invalid-tcp-hdr-length	Invalid tcp length	This counter is incremented when the security appliance receives a TCP packet whose size is smaller than the minimum-allowed header length or does not conform to the received packet length. **Recommendation**: The invalid packet could be a bogus packet being sent by an attacker. Investigate the traffic from the source in the following system message. **System log messages**: 500003.
invalid-udp-length	Invalid udp length	This counter is incremented when the security appliance receives a UDP packet whose size as calculated from the fields in the header is different from the measured size of the packet as received from the network. **Recommendation**: The invalid packet could be a bogus packet being sent by an attacker. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ipsec-clearpkt-notun	IPSEC Clear Pkt w/no tunnel	This counter will increment when the security appliance receives a packet that should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System log messages**: 402117
ipsec-ipv6	IPSEC via IPV6	This counter will increment when the security appliance receives an IPSec ESP packet, IPSec NAT-T ESP packet, or an IPSec over UDP ESP packet encapsulated in an IPv6 header. The security appliance does not currently support any IPSec sessions encapsulated in IPv6. **Recommendation**: None. **System log messages**: None.
ipsec-need-sa	IPSEC SA Not negotiated yet	This counter will increment when the security appliance receives a packet that requires encryption but has no established IPSec security association. This is generally a normal condition for LAN-to-LAN IPSec configurations. This indication will cause the security appliance to begin ISAKMP negotiations with the destination peer. **Recommendation**: If you have configured IPSec LAN-to-LAN on your security appliance, this indication is normal and does not indicate a problem. However, if this counter increments rapidly it may indicate a **crypto** configuration error or network error preventing the ISAKMP negotiation from completing. Verify that you can communicate with the destination peer and verify your **crypto** configuration using the **show running-config** command. **System log messages**: None.
ipsec-spoof	IPSEC Spoof detected	This counter will increment when the security appliance receives a packet which should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System log messages**: 402117

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ipsec-tun-down	IPSEC tunnel is down	This counter will increment when the security appliance receives a packet associated with an IPSec connection which is in the process of being deleted. **Recommendation**: This is a normal condition when the IPSec tunnel is torn down for any reason. **System log messages**: None.
ipsecudp-keepalive	IPSEC/UDP keepalive message	This counter will increment when the security appliance receives an IPSec over UDP keepalive message. IPSec over UDP keepalive messages are sent from the IPSec peer to the security appliance to keep NAT/PAT flow information current in network devices between the IPSec over UDP peer and the security appliance. **Note** These are not industry-standard NAT-T keepalive messages that are also carried over UDP and addressed to UDP port 4500. **Recommendation**: If you have configured IPSec over UDP on your security appliance, this indication is normal and does not indicate a problem. If IPSec over UDP is not configured on your security appliance, analyze your network traffic to determine the source of the IPSec over UDP traffic. **System log messages**: None.
ips-fail-close	IPS card is down	This counter is incremented and the packet is dropped when the AIP SSM is down and the **fail-close** option was used in IPS inspection. **Recommendation**: Check and bring up the AIP SSM. **System log messages**: 420001
ips-request	IPS Module requested drop	This counter is incremented and the packet is dropped as requested by the AIP SSM when the packet matches a signature on the IPS engine. **Recommendation**: Check System log messages and alerts on the AIP SSM. **System log messages**: 420002

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ipv6_sp-security-failed	IPv6 slowpath security checks failed	This counter is incremented and the packet is dropped for one of the following reasons: • An IPv6 through-the-box packet has the identical source and destination address. • An IPv6 through-the-box packet has a linklocal source or destination address. • An IPv6 through-the-box packet has a multicast destination address. **Recommendation**: These packets could indicate malicious activity, or could be the result of a misconfigured IPv6 host. Use the packet capture feature to capture type asp packets, and use the source MAC address to identify the source. **System log messages**: For identical source and destination address, system message 106016.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
l2_acl	FP L2 rule drop	This counter increments when the security appliance denies a packet due to an EtherType access list. The transparent mode security appliance permits the following traffic by default: • IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. **Note** For Layer 3 traffic travelling from a low to a high security interface, an extended access list is required on the low security interface. • ARPs are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic). **Note** The transparent mode security appliance does not pass CDP packets or IPv6 packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported. Packets permitted by EtherType access lists might still be dropped by an extended access list. The EtherType access list only supports EtherTypes and not Layer 2 destination MAC addresses. The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped. • TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF • IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF • BPDU multicast address equal to 0100.0CCC.CCCD • Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF **Recommendation**: If your non-IP packets are dropped by the security appliance, you can configure an EtherType access list to permit the Layer 2 traffic. **System log messages**: 106026, 106027

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
l2_same-lan-port	L2 Src/Dst same LAN port	This counter will increment when the security appliance or context is configured for transparent mode, and the security appliance determines that the destination interface's L2 MAC address is the same as its ingress interface. **Recommendation**: This is a normal condition when the security appliance or context is configured for transparent mode. Since the security appliance interface is operating in promiscuous mode, the security appliance or context receives all packets on the local LAN segment. **System log messages**: None.
loopback-buffer-full	Loopback buffer full	This counter is incremented and the packet is dropped when packets are sent from one context of the security appliance to another context through a shared interface, and there is no buffer space in the loopback queue. **Recommendation**: Check the system CPU to make sure it is not overloaded. **System log messages**: None.
lu-invalid-pkt	Invalid LU packet	The standby unit received a corrupted Logical Update packet. **Recommendation**: The packet corruption could be caused by a bad cable, interface card, line noise, or software defect. If the interface appears to be functioning properly, then report the problem to Cisco TAC. **System log messages**: None.
mp-pf-queue-full	Port Forwarding Queue Is Full	This counter is incremented when the Port Forwarding application's internal queue is full and it receives another packet for transmission. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-addr-renew-response	SVC Module received address renew response data frame	This counter will increment when the security appliance receives an Address Renew Response message from an SVC. The SVC should not be sending this message. **Recommendation**: This indicates that an SVC software error should be reported to the Cisco TAC. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
mp-svc-bad-framing	SVC Module received badly framed data	This counter will increment when the security appliance receives a packet from an SVC or the control software that it is unable to decode. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. The SVC or security appliance could be at fault. **System log messages**: 722037 (Only for SVC received data).
mp-svc-bad-length	SVC Module received bad data length	This counter will increment when the security appliance receives a packet from an SVC or the control software where the calculated and specified lengths do not match. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. The SVC or security appliance could be at fault. **System log messages**: 722037 (Only for SVC received data).
mp-svc-compress-error	SVC Module compression error	This counter will increment when the security appliance encounters an error during compression of data to an SVC. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. The SVC or security appliance could be at fault. **System log messages**: 722037
mp-svc-decompres-error	SVC Module decompression error	This counter will increment when the security appliance encounters an error during decompression of data from an SVC. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. The SVC or security appliance could be at fault. **System log messages**: 722037
mp-svc-delete-in-progress	SVC Module received data while connection was being deleted	This counter will increment when the security appliance receives a packet associated with an SVC connection that is in the process of being deleted. **Recommendation**: This is a normal condition when the SVC connection is torn down for any reason. If this error occurs repeatedly or in large numbers, it could indicate that clients are having network connectivity issues. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
mp-svc-flow-control	SVC Session is in flow control	This counter will increment when the security appliance needs to drop data because an SVC is temporarily not accepting any more data. **Recommendation**: This indicates that the client is unable to accept more data. The client should reduce the amount of traffic it is attempting to receive. **System log messages**: None.
mp-svc-invalid-mac	SVC Module found invalid L2 data in the frame	This counter will increment when the security appliance is finds an invalid L2 MAC header attached to data received from an SVC. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-invalid-mac-len	SVC Module found invalid L2 data length in the frame	This counter will increment when the security appliance is finds an invalid L2 MAC length attached to data received from an SVC. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-no-channel	SVC Module does not have a channel for reinjection	This counter will increment when the interface that the encrypted data was received upon cannot be found in order to inject the decrypted data. **Recommendation**: If an interface is shut down during a connection, this could happen; re-enable/check the interface. Otherwise, this indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-no-fragment	SVC Module unable to fragment packet:	This counter is incremented when a packet to be sent to the SVC is not permitted to be fragmented or when there are not enough data buffers to fragment the packet. **Recommendation**: Increase the MTU of the SVC to reduce fragmentation. Avoid using applications that do not permit fragmentation. Decrease the load on the device to increase available data buffers. **System log messages**: None.
mp-svc-no-mac	SVC Module unable to find L2 data for frame	This counter will increment when the security appliance is unable to find an L2 MAC header for data received from an SVC. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
mp-svc-no-prepend	SVC Module does not have enough space to insert header	This counter will increment when there is not enough space before the packet data to prepend a MAC header in order to put the packet onto the network. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-no-session	SVC Module does not have a session	This counter will increment when the security appliance cannot determine the SVC session that this data should be transmitted over. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
mp-svc-unknown-type	SVC Module received unknown data frame	This counter will increment when the security appliance receives a packet from an SVC where the data type is unknown. **Recommendation**: Validate that the SVC being used by the client is compatible with the version of security appliance software. **System log messages**: None.
natt-keepalive	NAT-T keepalive message	This counter will increment when the security appliance receives an IPSec NAT-T keepalive message. NAT-T keepalive messages are sent from the IPSec peer to the security appliance to keep NAT/PAT flow information current in network devices between the NAT-T IPSec peer and the security appliance. **Recommendation**: If you have configured IPSec NAT-T on your security appliance, this indication is normal and does not indicate a problem. If NAT-T is not configured on your security appliance, analyze your network traffic to determine the source of the NAT-T traffic. **System log messages**: None
no-adjacency	No valid adjacency	This counter is incremented when the security appliance has tried to obtain an adjacency and could not obtain the MAC address for the next hop. The packet is dropped. **Recommendation**: Configure a capture for this drop reason and check if a host with the specified destination address exists on the connected network or is routable from the security appliance. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
no-mcast-entry	FP no mcast entry	This counter increments because of one of the following reasons: • A packet has arrived that matches a multicast flow, but the multicast service is no longer enabled, or was re-enabled after the flow was built. **Recommendation**: Reenable multicast if it is disabled. **System log messages**: None. • A multicast entry change has been detected after a packet was punted to the CP, and the NP can no longer forward the packet since no entry is present. **Recommendation**: None. **System log messages**: None.
no-mcast-intrf	FP no mcast output intrf	This counter increments because of one of the following reasons: • All output interfaces have been removed from the multicast entry. **Recommendation**: Verify that there are no longer any receivers for this group. **System log messages**: None. • The multicast packet could not be forwarded. **Recommendation**: Verify that a flow exists for this packet. **System log messages**: None.
non-ip-pkt-in-routed-mode	Non-IP packet received in routed mode	This counter will increment when the security appliance receives a packet that is not an IPv4, IPv6, or ARP packet, and the security appliance or context is configured for routed mode. In normal operation such packets should be dropped. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: 106026, 106027
no-route	No route to host	This counter is incremented when the security appliance tries to send a packet out of an interface and does not find a route for it in the routing table. **Recommendation**: Verify that a route exists for the destination address obtained from the generated system message. **System log messages**: 110001

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
np-socket-closed	Dropped pending packets in a closed socket	If a socket is abruptly closed, by the user or software, then any pending packets in the pipeline for that socket are also dropped. This counter is incremented for each packet in the pipeline that is dropped. **Recommendation**: It is common to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further. **System log messages**: None.
np-sp-invalid-spi	Invalid SPI	This counter increments when the security appliance receives an IPSec ESP packet addressed to the security appliance that specifies an SPI (security parameter index) not currently known by the security appliance. **Recommendation**: Occasional invalid SPI indications are common, especially during rekey processing. Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing a high rate of invalid SPI indications, analyze your network traffic to determine the source of the ESP traffic. **System log messages**: 402114
punt-rate-limit	Punt rate limit exceeded	This counter will increment when the security appliance attempts to forward a Layer 2 packet to a rate-limited control point service routine, and the rate limit (per/second) is now being exceeded. Currently, the only Layer 2 packets destined for a control point service routine that are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second per interface. **Recommendation**: Analyze your network traffic to determine the reason behind the high rate of ARP packets. **System log messages**: 322002, 322003
queue-removed	Queued packet dropped	When the QoS configuration is changed or removed, the existing packets in the output queues awaiting transmission are dropped and this counter is incremented. **Recommendation**: Under normal conditions, this may be seen when the QoS configuration has been changed by the user. If this occurs when no changes to the QoS configuration were performed, please contact Cisco TAC. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
rate-exceeded	QoS rate exceeded	This counter is incremented when rate-limiting (policing) is configured on an egress/ingress interface, and the egress/ingress traffic rate exceeds the burst rate configured. The counter is incremented for each packet dropped. **Recommendation**: Investigate and determine why the rate of traffic leaving the interface is higher than the configured rate. This may be normal, or could be an indication of virus or attempted attack. **System log messages**: None.
rm-conn-limit	RM connection limit reached	This counter is incremented when the maximum number of connections for a context or the system has been reached, and a new connection is attempted. **Recommendation**: The device administrator can use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and "Denied" counts and adjust resource limits if desired. **System log messages**: 321001
rm-conn-rate-limit	RM connection rate limit reached	This counter is incremented when the maximum connection rate for a context or the system has been reached and a new connection is attempted. **Recommendation**: The device administrator can use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and "Denied" counts and adjust resource limits if desired. **System log messages**: 321002
rpf-violated	Reverse-path verify failed	This counter is incremented when **ip verify reverse-path** is configured on an interface and the security appliance receives a packet for which the route lookup of the source IP did not yield the same interface as the one on which the packet was received. **Recommendation**: Trace the source of traffic based on the source IP printed in the system message below, and investigate why it is sending spoofed traffic. **System log messages**: 106021

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
security-failed	Early security checks failed	This counter is incremented and the packet is dropped when the security appliance: • Receives an IPv4 multicast packet when the packet multicast MAC address does not match the packet multicast destination IP address • Receives an IPv6 or IPv4 teardrop fragment containing either small offset or fragment overlapping • Receives an IPv4 packet that matches an IP audit signature **Recommendation**: Contact the remote peer administrator or escalate this issue according to your security policy. For detailed description and System log messages for IP audit attack checks please refer the **ip audit signature** command. **System log messages**: 106020, 400xx in case of IP audit checks
send-ctm-error	Send to CTM returned error	This counter is obsolete in the security appliance and should never increment. **Recommendation**: None. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
sp-security-failed	Slowpath security checks failed	This counter is incremented and the packet is dropped when the security appliance: • Is in routed mode and receives a through-the-box: – L2 broadcast packet – IPv4 packet with destination IP address equal to 0.0.0.0 – IPv4 packet with source IP address equal to 0.0.0.0 **Recommendation**: Determine if an external user is trying to compromise the protected network. Check for misconfigured clients. **System log messages**: 106016 • Is in routed or transparent mode and receives a through-the-box IPv4 packet with: – The first octet of the source IP address is equal to zero – The source IP address is equal to the loopback IP address – Network part of the source IP address is equal to all 0s – The network part of the source IP address is equal to all 1s – The source IP address host part is equal to all 0s or all 1s **Recommendation**: Determine if an external user is trying to compromise the protected network. Check for misconfigured clients. **System log messages**: 106016 • In routed or transparent mode and receives an IPv4 or IPv6 packet with the same source and destination IP addresses **Recommendation**: If this message counter is incrementing rapidly, an attack may be in progress. Use the packet capture feature to capture type asp packets, and check the source MAC address in the packet to see where they are coming from. **System log messages**: 106017

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ssm-app-fail	Service module is down	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a packet to be inspected by the SSM is dropped because the SSM has become unavailable. Some examples of this are: software or hardware failure, software or signature upgrade, or the module being shut down. **Recommendation**: The SSM manager process running in the security appliance control plane would have issued system messages and CLI warning to inform you of the failure. Please consult the documentation that comes with the SSM to troubleshoot the SSM failure. Contact Cisco TAC if needed. **System log messages**: None.
ssm-app-request	Service module requested drop	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when the application running on the SSM requests the security appliance to drop a packet. **Recommendation**: More information could be obtained by querying the incident report or system messages generated by the SSM itself. Please consult the documentation that comes with your SSM for instructions. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ssm-asdp-invalid	Invalid ASDP packet received from SSM card	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when the security appliance receives an ASA SSM Dataplane Protocol (ASDP) packet from the internal data plane interface, but the driver encountered a problem when parsing the packet. ASDP is a protocol used by the security appliance to communicate with certain types of SSMs, like the CSC SSM. This could happen for various reasons, for example: the ASDP protocol version is not compatible between the security appliance and the SSM, in which case the SSM manager process in the control plane issues system messages and CLI warnings to inform you of the proper version of images that needs to be installed; the ASDP packet belongs to a connection that has already been terminated on the security appliance; the security appliance has switched to the standby state (if failover is enabled) in which case it can no longer pass traffic; or any unexpected value when parsing the ASDP header and payload. **Recommendation**: The counter is usually 0 or a very small number. But you should not be concerned if the counter slowly increases over time, especially when there has been a failover, or you have manually cleared connections on the security appliance via the CLI. If the counter increases drastically during normal operation, please contact Cisco TAC. System log messages: 421003, 421004
ssm-dpp-invalid	Invalid packet received from SSM card	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when the security appliance receives a packet from the internal data plane interface but could not find the proper driver to parse it. **Recommendation**: The data plane driver is dynamically registered depending on the type of SSM installed in the system. So this could happen if data plane packets arrive before the security appliance is fully initialized. This counter is usually 0. You should not be concerned if there are a few drops. However, if this counter keeps rising when system is up and running, it may indicate a problem. Please contact Cisco TAC if you suspect it affects the normal operation of your the security appliance. **System log messages**: None.
tcp_xmit_partial	TCP retransmission partial	This counter is incremented and the packet is dropped when the **check-retransmission** feature is enabled, and a partial TCP retransmission was received. **Recommendation**: None. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-3whs-failed	TCP failed 3 way handshake	This counter is incremented and the packet is dropped when security appliance receives an invalid TCP packet during the three-way handshake. For example, the SYN-ACK from a client will be dropped for this reason. **Recommendation**: None. **System log messages**: None.
tcp-acked	TCP DUP and has been ACKed	This counter is incremented and the packet is dropped when the security appliance receives a retransmitted data packet and the data has been acknowledged by the peer TCP endpoint. **Recommendation**: None. **System log messages**: None.
tcp-ack-syn-diff	TCP ACK in SYNACK invalid	This counter is incremented and the packet is dropped when the security appliance receives a SYN-ACK packet during the three-way handshake with an incorrect TCP acknowledgement number. **Recommendation**: None. **System log messages**: None.
tcp-bad-option-len	Bad option length in TCP	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a TCP option set, but the option length does not match the length defined for that option in the TCP RFC. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.
tcp-bad-option-list	TCP option list invalid	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a non-standard TCP header option. **Recommendation**: To allow such TCP packets or clear non-standard TCP header options and then allow the packet, use the **tcp-options** command. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-bad-sack-allow	Bad TCP SACK ALLOW option	This counter is incremented and the packet is dropped when the appliance receives a TCP packet with the selective acknowledgement option, but the SYN flag is not set. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.
tcp-bad-winscale	Bad TCP window scale value	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with the window-scale option greater than 14. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.
tcp-buffer-full	TCP packet buffer full	This counter is incremented and the packet is dropped when the security appliance receives an out-of-order TCP packet on a connection, and there is no buffer space to store this packet. Typically TCP packets are put into order on connections that are inspected by the security appliance or when packets are sent to an SSM for inspection. There is a default queue size, and when packets in excess of this default queue size are received they will be dropped. **Recommendation**: On ASA platforms the queue size could be increased using the **queue-limit** command. **System log messages**: None.
tcp-conn-limit	TCP Connection limit reached	This reason is given for dropping a TCP packet during the TCP connection establishment phase when the connection limit has been exceeded. The connection limit is configured using the **set connection conn-max** command. **Recommendation**: If this is incrementing rapidly, check the System log messages to determine which host's connection limit is reached. The connection limit may need to be increased if the traffic is normal, or the host may be under attack. **System log messages**: 201011
tcp-data-past-fin	TCP data send after FIN	This counter is incremented and the packet is dropped when the security appliance receives new a TCP data packet from an endpoint which had sent a FIN to close the connection. **Recommendation**: None. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-discarded-ooo	TCP ACK in 3 way handshake invalid	This counter is incremented and the packet is dropped when the security appliance receives a TCP ACK packet from a client during the three-way-handshake and the sequence number is not the next expected sequence number. **Recommendation**: None. **System log messages**: None.
tcp-dual-open	TCP Dual open denied	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet from the server and an embryonic TCP connection is already open. **Recommendation**: None. **System log messages**: None.
tcp-fo-drop	TCP replicated flow pak drop	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a control flag like SYN, FIN, or RST on an established connection just after the security appliance has taken over as active unit. **Recommendation**: None. **System log messages**: None.
tcp-invalid-ack	TCP invalid ACK	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with an acknowledgement number greater than the data sent by the peer TCP endpoint. **Recommendation**: None. **System log messages**: None.
tcp-mss-exceeded	TCP data exceeded MSS	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a data length greater than the MSS advertised by the peer TCP endpoint. **Recommendation**: To allow such TCP packets, use the **exceed-mss** command. **System log messages**: 4419001
tcpnorm-rexmit-bad	TCP bad retransmission	This counter is incremented and the packet is dropped when the **check-retransmission** feature is enabled, and a TCP retransmission with different data from the original packet was received. **Recommendation**: None. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcpnorm-win-variation	TCP unexpected window size variation	This counter is incremented and the packet is dropped when the window size advertised by the TCP endpoint is drastically changed without accepting that much data. **Recommendation**: To allow such packet, use the **window-variation** command. **System log messages**: None.
tcp-not-syn	First TCP packet not SYN	The security appliance received a non-SYN packet as the first packet of a non-intercepted and non-nailed connection. **Recommendation**: Under normal conditions, this may be seen when the security appliance has already closed a connection, and the client or server still believe the connection is open, and continue to transmit data. Some examples where this may occur is just after a **clear local-host** or **clear xlate** command is issued. Also, if connections have not been recently removed, and the counter is incrementing rapidly, the security appliance may be under attack. Capture a sniffer trace to help isolate the cause. **System log messages**: 6106015
tcp-paws-fail	TCP packet failed PAWS test	This counter is incremented and the packet is dropped when a TCP packet with a timestamp header option fails the PAWS (Protect Against Wrapped Sequences) test. **Recommendation**: To allow such connections to proceed, use the **tcp-options** command to clear the timestamp option. **System log messages**: None.
tcp-reserved-set	TCP reserved flags set	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with reserved flags set in TCP header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. To allow such TCP packets or clear reserved flags and then pass the packet, use the **reserved-bits** command. **System log messages**: None
tcp-rstfin-ooo	TCP RST/FIN out of order	This counter is incremented and the packet is dropped when the security appliance receives a RST or a FIN packet with the incorrect TCP sequence number. **Recommendation**: None. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-rst-syn-in-win	TCP RST/SYN in window	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN or TCP RST packet on an established connection with a sequence number within the window, but not as the next expected sequence number. **Recommendation**: None. **System log messages**: None.
tcp-seq-past-win	TCP packet SEQ past window	This counter is incremented and the packet is dropped when the security appliance receives a TCP data packet with a sequence number beyond the window allowed by the peer TCP endpoint. **Recommendation**: None. **System log messages**: None.
tcp-seq-syn-diff	TCP SEQ in SYN/SYNACK invalid	This counter is incremented and the packet is dropped when the security appliance receives a SYN or SYN-ACK packet during the three-way handshake with an incorrect TCP sequence number. **Recommendation**: None. **System log messages**: None.
tcp-synack-data	TCP SYNACK with data	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN-ACK packet with data. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.
tcp-synack-ooo	TCP SYNACK on established conn	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN-ACK packet on an established TCP connection. **Recommendation**: None. **System log messages**: None.
tcp-syn-data	TCP SYN with data	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet with data. **Recommendation**: To allow such TCP packets use the **syn-data** command. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-syn-ooo	TCP SYN on established conn	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet on an established TCP connection. **Recommendation**: None. **System log messages**: None.
tcp-winscale-no-syn	TCP Window scale on non-SYN	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with the window-scale TCP option without SYN flag set. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: None.
telnet-not-permitted	Telnet not permitted on least secure interface	This counter is incremented and packet is dropped when the appliance receives a TCP SYN packet attempting to establish a TELNET session to the appliance and that packet was received on the least secure interface. **Recommendation**: To establish a TELNET session to the appliance via the least secure interface, first establish an IPSec tunnel to that interface and then connect the TELNET session over that tunnel. **System log messages**: 402117
tfw-no-mgmt-ip-config	No management IP address configured for TFW	This counter is incremented when the security appliance receives an IP packet in transparent mode and has no management IP address defined. The packet is dropped. **Recommendation**: Configure the security appliance with a management IP address and mask values. **System log messages**: 322004
unable-to-add-flow	Flow hash full	This counter is incremented when a newly created flow is inserted into the flow hash table, and the insertion failed because the hash table was full. The flow and the packet are dropped. This is different from the counter that increments when the maximum connection limit is reached. **Recommendation**: This message signifies a lack of resources on the security appliance to support an operation that should have been successful. Please check if the connections in the **show conn** output have exceeded their configured idle timeout values. If so, contact Cisco TAC. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
unable-to-create-flow	Flow denied due to resource limitation	This counter is incremented and the packet is dropped when flow creation fails due to a system resource limitation. The resource limit may be either: • System memory • Packet block extension memory • System connection limit The first two causes occur simultaneously with flow drop reason "No memory to complete flow." **Recommendation**: • Observe if free system memory is low. • Observe if flow drop reason "No memory to complete flow" occurs. • Observe if the connection count reaches the system connection limit using the **show resource usage** command. **System log messages**: None.
unexpected-packet	Unexpected packet	This counter is incremented when the security appliance in transparent mode receives a non-IP packet destined to its MAC address, but there is no corresponding service running on the security appliance to process the packet. Recommendation: Verify if the security appliance is under attack. If there are no suspicious packets, or the security appliance is not in transparent mode, this counter is most likely being incremented due to a software error. Attempt to capture the traffic that is causing the counter to increment and contact the Cisco TAC. **System log messages**: None.
unsupported-ip-version	Unsupported IP version	This counter is incremented when the security appliance receives an IP packet that has an unsupported version in the version field of the IP header. Specifically, if the packet does not belong to version 4 or version 6, the packet is dropped. **Recommendation**: Verify that other devices on the connected network are configured to send IP packets belonging to versions 4 or 6 only. **System log messages**: None.

Table 25-1 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
unsupport-ipv6-hdr	Unsupported IPV6 header	This counter is incremented and the packet is dropped if an IPv6 packet is received with an unsupported IPv6 extension header. The supported IPv6 extension headers are: TCP, UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment. The IPv6 routing extension header is not supported, and any extension header not listed above is not supported. IPv6 ESP and AH headers are supported only if the packet is through-the-box. To-the-box IPv6 ESP and AH packets are not supported and will be dropped. **Recommendation**: This error may be due to a misconfigured host. If this error occurs repeatedly or in large numbers, it could also indicate spurious or malicious activity such as an attempted DoS attack. **System log messages**: None.
vpn-context-expired	Expired VPN context	This counter will increment when the security appliance receives a packet that requires encryption or decryption, and the ASP VPN context required to perform the operation is no longer valid. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None
wccp-redirect-no-route	No route to Cache Engine	This counter is incremented when the security appliance tries to redirect a packet and does not find a route to the Cache Engine. **Recommendation**: Verify that a route exists for Cache Engine. **System log messages**: None
wccp-return-no-route	No route to host for WCCP returned packet	This counter is incremented when a packet is returned from the Cache Engine and the security appliance does not find a route for the original source of the packet. **Recommendation**: Verify that a route exists for the source IP address of the packet returned from Cache Engine. **System log messages**: None

Table 25-2 lists valid values for the *flow_drop_reason* argument for dropped flows.

Table 25-2 Flow Drop Reasons

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
acl-drop	Flow is denied by access rule	This counter is incremented when a packet is denied by the security appliance, and flow creation is denied. The deny rule could be a default rule created when the security appliance comes up, when various features are turned on or off, when an access list is applied to an interface, or any other feature. Apart from default rule drops, a flow could be denied because of: • An access list configured on an interface • An access list configured for AAA, and AAA denied the user • Through traffic arriving at a management-only interface • Unencrypted traffic arriving on a IPSec-enabled interface • Implicit deny at the end of an access list **Recommendation**: Observe if one of System log messages related to packet drop display. Flow drop results in the corresponding packet drop that would trigger the requisite system message. **System log messages**: None.
audit-failure	Audit failure	A flow was freed after matching an **ip audit** signature that had reset as the associated action. **Recommendation**: If removing the flow is not the desired outcome of matching this signature, then remove the reset action from the **ip audit** command. **System log messages**: None.
closed-by-inspection	Flow closed by inspection	This reason is given for closing a flow due to an error detected during application inspection. For example, if an error is detected during inspecting an H323 message, the corresponding H323 flow is closed with this reason. **Recommendation**: None. **System log messages**: None.
conn-limit-exceeded	Connection limit exceeded	This reason is given for closing a flow when the connection limit has been exceeded. The connection limit is configured using the **set connection conn-max** command. **Recommendation**: None. **System log messages**: 201011
fin-timeout	FIN Timeout	This reason is given for closing a TCP flow due to expiry of half-closed timer. **Recommendation**: If these are valid sessions which take longer to close a TCP flow, increase the half-closed timeout. **System log messages**: 302014

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
flow-reclaimed	Non-tcp/udp flow reclaimed for new request	This counter is incremented when a reclaimable flow is removed to make room for a new flow. This occurs only when the number of flows through the security appliance equals the maximum number permitted by the software imposed limit, and a new flow request is received. When this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels permitted by the security appliance, then the oldest reclaimable flow is removed to make room for the new flow. All flows except the following are deemed to be reclaimable: • TCP, UDP, GRE and failover flows • ICMP flows if ICMP stateful inspection is enabled • ESP flows to the security appliance **Recommendation**: No action is required if this counter is incrementing slowly. If this counter is incrementing rapidly, it could mean that the security appliance is under attack and the security appliance is spending more time reclaiming and rebuilding flows. **System log messages**: 302021
fo-primary-closed	Failover primary closed	The standby unit received a flow delete message from the active unit and terminated the flow. **Recommendation**: If the security appliance is running stateful failover, then this counter should increment for every replicated connection that is torn down on the standby appliance. **System log messages**: 302014, 302016, 302018
fo-standby	Flow closed by failover standby	If a through-the-box packet arrives at the security appliance or a context that is in a standby state, then a flow is created, the packet is dropped, and the flow removed. This counter will increment each time a flow is removed in this manner. **Recommendation**: This counter should never be incrementing on the active security appliance or context. However, it is normal to see it increment on the standby security appliance or context. **System log messages**: 302014, 302016, 302018
fo_rep_err	Standby flow replication error	The standby unit failed to replicate a flow. **Recommendation**: If the security appliance is processing VPN traffic, then this counter could be constantly increasing on the standby unit because the flow could be replicated before the IKE SA information. No action is required in this case. If the appliance is not processing VPN traffic, then this indicates a software detect; turn on the **debug fover fail** command on the standby unit, collect the debug output, and report the problem to Cisco TAC. **System log messages**: 302014, 302016, 302018

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
host-removed	Host is removed	The flow was removed in response to the **clear local-host** command. **Recommendation**: This is an information counter. **System log messages**: 302014, 302016, 302018, 302021, 305010, 305012, 609002
inspect-fail	Inspection failure	This counter will increment when the security appliance fails to enable protocol inspection carried out by the NP for the connection. The cause could be memory allocation failure, or for ICMP error message, the security appliance not being able to find any established connection related to the frame embedded in the ICMP error message. **Recommendation**: Check system memory usage. For the ICMP error message, if the cause is an attack, you can deny the host using the access lists. **System log messages**: 313004 for ICMP error.
ips-fail-close	IPS fail-close	This reason is given for terminating a flow because the AIP SSM is down and the fail-close option was used with IPS inspection. **Recommendation**: Check and bring up the AIP SSM. **System log messages**: 420001
ips-request	Flow terminated by IPS	This reason is given for terminating a flow as requested by the AIP SSM. **Recommendation**: Check System log messages and alerts on the AIP SSM. **System log messages**: 420002
ipsec-selector-failure	IPSec VPN inner policy selector mismatch detected	This counter is incremented when an IPsec packet is received with an inner IP header that does not match the configured policy for the tunnel. **Recommendation**: Verify that the crypto access lists for the tunnel are correct and that all acceptable packets are included in the tunnel identity. Verify that the security appliance is not under attack if this message is repeatedly seen. **System log messages**: 402116
ipsec-spoof-detect	IPsec spoof packet detected	This counter will increment when the security appliance receives a packet that should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System log messages**: 402117

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
loopback	Flow is a loopback	This reason is given for closing a flow due to the following conditions: • U-turn traffic is present on the flow. • **same-security-traffic permit intra-interface** is not configured. **Recommendation**: To allow U-turn traffic on an interface, configure the interface with the **same-security-traffic permit intra-interface** command. **System log messages**: None.
mcast-entry-removed	Multicast entry removed	This reason is given for one of the following cases: • A packet has arrived that matches a multicast flow, but the multicast service is no longer enabled, or was re-enabled after the flow was built. **Recommendation**: Reenable multicast if it is disabled. **System log messages**: None. • The multicast entry has been deleted so the flow is being cleaned up, but the packet will be reinjected into the data path. **Recommendation**: None. **System log messages**: None.
mcast-intrf-removed	Multicast interface removed	This reason is given for one of the following cases: • An output interface has been removed from the multicast entry. **Recommendation**: None. **System log messages**: None. • All output interfaces have been removed from the multicast entry. **Recommendation**: Verify that there are no longer any receivers for this group. **System log messages**: None.
nat-failed	NAT failed	Failed to create an xlate to translate an IP or transport header. **Recommendation**: If NAT is not desired, disable **nat-control**. Otherwise, use the **static**, **nat**, or **global** command to configure NAT policy for the dropped flow. For dynamic NAT, ensure that each **nat** command is paired with at least one **global** command. Use **show running-config nat** and **debug pix process** to verify NAT rules. **System log messages**: 305005, 305006, 305009, 305010, 305011, 305012

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
nat-rpf-failed	NAT reverse path failed	Rejected attempt to connect to a mapped host using the mapped host's real address. **Recommendation**: When not on the same interface as the host undergoing NAT, use the mapped address instead of the real address to connect to the host. Also, enable the appropriate **inspect** command if the application embeds the IP address. **System log messages**: 305005
need-ike	Need to start IKE negotiation	This counter will increment when the security appliance receives a packet that requires encryption but has no established IPSec security association. This is generally a normal condition for LAN-to-LAN IPSec configurations. This indication will cause the security appliance to begin ISAKMP negotiations with the destination peer. **Recommendation**: If you have configured IPSec LAN-to-LANs on your security appliance, this indication is normal and does not indicate a problem. However, if this counter increments rapidly, it may indicate a **crypto** configuration error or network error preventing the ISAKMP negotiation from completing. Verify that you can communicate with the destination peer and verify your **crypto** configuration using the **show running-config** command. **System log messages**: None.
no-inspect	Failed to allocate inspection	This counter will increment when the security appliance fails to allocate a run-time inspection data structure upon connection creation. The connection will be dropped. **Recommendation**: This error condition is caused when the security appliance runs out of system memory. Please check the current available free memory by executing the **show memory** command. **System log messages**: None.
no-ipv6-ipsec	IPsec over IPv6 unsupported	This counter will increment when the security appliance receives an IPSec ESP packet, IPSec NAT-T ESP packet, or an IPSec over UDP ESP packet encapsulated in an IPv6 header. The security appliance does not currently support any IPSec sessions encapsulated in IPv6. **Recommendation**: None. **System log messages**: None.
non_tcp_syn	non-syn TCP	This reason is given for terminating a TCP flow when the first packet is not a SYN packet. **Recommendation**: None. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
out-of-memory	No memory to complete flow	This counter is incremented when the security appliance is unable to create a flow because of insufficient memory. **Recommendation**: Verify that the security appliance is not under attack by checking the current connections. Also verify if the configured timeout values are too large resulting in idle flows residing in memory longer. Check the free memory available by issuing the **show memory** command. If free memory is low, issue the **show processes memory** command to determine which processes are utilizing most of the memory. **System log messages**: None.
parent-closed	Parent flow is closed	When the parent flow of a subordinating flow is closed, the subordinating flow is also closed. For example, an FTP data flow (subordinating flow) will be closed with this specific reason when its control flow (parent flow) is terminated. This reason is also given when a secondary flow (pin-hole) is closed by its controlling application. For example, when the BYE messaged is received, the SIP inspection engine (controlling application) will close the corresponding SIP RTP flows (secondary flow). **Recommendation**: None. **System log messages**: None.
pinhole-timeout	Pinhole timeout	This counter is incremented to report that the security appliance opened a secondary flow, but no packets passed through this flow within the timeout interval, and hence it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel. **Recommendation**: None. **System log messages**: 302014, 302016
recurse	Close recursive flow	A flow was recursively freed. This reason applies to pair flows and multicast slave flows, and serves to prevent System log messages being issued for each of these subordinate flows. **Recommendation**: None. **System log messages**: None.
reinject-punt	Flow terminated by punt action	This counter is incremented when a packet is punted to the exception path for processing by one of the enhanced services such as inspection or AAA. The servicing routine, having detected a violation in the traffic flowing on the flow, requests that the flow be dropped. The flow is immediately dropped. **Recommendation**: Please watch for System log messages triggered by a servicing routine. Flow drop terminates the corresponding connection. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
reset-by-ips	Flow reset by IPS	This reason is given for terminating a TCP flow as requested by the AIP SSM. **Recommendation**: Check System log messages and alerts on the AIP SSM. **System log messages**: 420003
reset-in	TCP Reset-I	This reason is given for closing an outbound flow (from a low-security interface to a same- or high-security interface) when a TCP reset is received on the flow. **Recommendation**: None. **System log messages**: 302014
reset-out	TCP Reset-O	This reason is given for closing an inbound flow (from a high-security interface to low-security interface) when a TCP reset is received on the flow. **Recommendation**: None. **System log messages**: 302014
shunned	Flow shunned	This counter will increment when a packet is received that has a source IP address that matches a host in the shun database. When a **shun** command is applied, it will be incremented for each existing flow that matches the **shun** command. **Recommendation**: None. **System log messages**: 401004
ssl-bad-record-detect	SSL bad record detected	This counter is incremented for each unknown SSL record type received from the remote peer. Any unknown record type received from the peer is treated as a fatal error and the SSL connections that encounter this error must be terminated. **Recommendation**: It is not normal to see this counter increment at any time. If this counter is incremented, it usually means that the SSL protocol state is out of sync with the client software. The most likely cause of this problem is a software defect in the client software. Contact the Cisco TAC with the client software or web browser version and provide a network trace of the SSL data exchange to troubleshoot this problem. **System log messages**: None.
ssl-handshake-failed	SSL handshake failed	This counter is incremented when the TCP connection is dropped because the SSL handshake failed. **Recommendation**: This is to indicate that the TCP connection is dropped because the SSL handshake failed. If the problem cannot be resolved based on the System log messages information generated by the handshake failure condition, please include the related System log messages information when contacting the Cisco TAC. **System log messages**: 725006, 725014

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
rm-xlate-limit	RM xlate limit reached	This counter is incremented when the maximum number of xlates for a context or the system has been reached and a new connection is attempted. **Recommendation**: The device administrator can use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and "Denied" counts and adjust resource limits if desired. **System log messages**: 321001
rm-host-limit	RM host limit reached	This counter is incremented when the maximum number of hosts for a context or the system has been reached and a new connection is attempted. **Recommendation**: The device administrator can use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and "Denied" counts and adjust resource limits if desired. **System log messages**: 321001
rm-inspect-rate-limit	RM inspect rate limit reached	This counter is incremented when the maximum inspection rate for a context or the system has been reached and a new connection is attempted. **Recommendation**: The device administrator can use the commands **show resource usage** and **show resource usage system** to view context and system resource limits and "Denied" counts and adjust resource limits if desired. **System log messages**: 321002
ctm-crypto-request-error	CTM crypto request error	This counter is incremented each time CTM cannot accept our crypto request. This usually means the crypto hardware request queue is full. **Recommendation**: Issue the show crypto protocol statistics ssl command and contact the Cisco TAC with this information. **System log messages**: None.
ssl-record-decrypt-error	SSL record decryption failed	This counter is incremented when a decryption error occurs during SSL data receive. This usually means that there is a bug in the SSL code of the ASA or peer, or an attacker may be modifying the data stream. The SSL connection has been closed. **Recommendation**: Investigate the SSL data streams to and from your ASA. If there is no attacker, then this indicates a software error that should be reported to the Cisco TAC. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
np-midpath-service-failure	NP midpath service failure	This is a general counter for critical midpath service errors. **Recommendation**: This indicates that a software error should be reported to Cisco TAC. **System log messages**: None.
np-socket-conn-not-accepted	A new socket connection was not accepted	This counter is incremented for each new socket connection that is not accepted by the security appliance. **Recommendation**: It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further. **System log messages**: None.
np-socket-failure	NP socket failure	This is a general counter for critical socket processing errors. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
np-socket-data-move-failure	NP socket data movement failure	This counter is incremented for socket data movement errors. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
np-socket-new-conn-failure	NP socket new connection failure	This counter is incremented for new socket connection failures. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.
np-socket-transport-closed	NP socket transport closed	This counter is incremented when the transport attached to the socket is abruptly closed. **Recommendation**: It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of socket-based applications, then this may be caused by a software defect. Contact the Cisco TAC to investigate the issue further. **System log messages**: None.
np-socket-block-conv-failure	NP socket block conversion failure	This counter is incremented for socket block conversion failures. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
ssl-received-close-alert	SSL received close alert	This counter is incremented each time the security appliance receives a close alert from the remote client. This indicates that the client has notified us they are going to drop the connection. It is part of the normal disconnect process. **Recommendation**: None. **System log messages**: 725007.
tracer-flow	Packet-tracer traced flow drop	This counter is internally used by packet-tracer for flow freed once tracing is complete. **Recommendation**: None. **System log messages**: None.
ssl-malloc-error	SSL malloc error	This counter is incremented for each malloc failure that occurs in the SSL lib. This is to indicate that SSL encountered a low memory condition where it can't allocate a memory buffer or packet block. **Recommendation**: Check the security appliance memory and packet block condition and contact Cisco the TAC with this memory information. **System log messages**: None.
ssm-app-fail	Service module failed	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a connection that is being inspected by the SSM is terminated because the SSM has failed. **Recommendation**: The card manager process running in the security appliance control plane issued system messages and CLI warning to inform you of the failure. Please consult the documentation that comes with the SSM to trouble shoot the SSM failure. Contact Cisco TAC if needed. **System log messages**: 421001
ssm-app-incompetent	Service module incompetent	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when a connection is supposed to be inspected by the SSM, but the SSM is not able to inspect it. This counter is reserved for future use. It should always be 0 in the current release. **Recommendation**: None. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
ssm-app-request	Flow terminated by service module	This counter only applies to the ASA 5500 series adaptive security appliance. It is incremented when the application running on the SSM requests the security appliance to terminate a connection. **Recommendation**: You can obtain more information by querying the incident report or system messages generated by the SSM itself. Please consult the documentation that comes with comes with the SSM for instructions. **System log messages**: None.
svc-failover	An SVC socket connection is being disconnected on the standby unit	This counter is incremented for each new SVC socket connection that is disconnected when the active unit is transitioning into standby state as part of a failover transition. **Recommendation**: None. This is part of a normal cleanup of a SVC connection when the current device is transitioning from active to standby. Existing SVC connections on the device are no longer valid and need to be removed. **System log messages**: None.
svc-replacement-conn	SVC replacement connection established	This counter is incremented when an SVC connection is replaced by a new connection. **Recommendation**: None. This may indicate that users are having difficulty maintaining connections to the security appliance. Users should evaluate the quality of their home network and Internet connection. **System log messages**: 722032
svc-spoof-detect	SVC spoof packet detected	This counter will increment when the security appliance receives a packet which should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established SVC connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed SVC traffic. **System log messages**: None.
syn-timeout	SYN Timeout	This reason is given for closing a TCP flow due to expiry of embryonic timer. **Recommendation**: If these are valid sessions that take longer to establish a connection, then increase the embryonic timeout. **System log messages**: 302014

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
tcp-fins	TCP FINs	This reason is given for closing a TCP flow when TCP FIN packets are received. **Recommendation**: This counter will increment for each TCP connection that is terminated normally with FINs. **System log messages**: 302014
tcp-intercept-no-response	TCP intercept server no respond	SYN retransmission timeout after trying three times, once every second. Server unreachable, tearing down connection. **Recommendation**: Check if the server is reachable from the security appliance. **System log messages**: None.
tcp-intercept-kill	Flow terminated by TCP Intercept	TCP intercept tore down the connection for the following reasons: 1. This is the first SYN 2. A connection is created for the SYN 3. TCP intercept replied with a SYN cookie; or TCP intercept sends a SYN to the server and the server replies with a RST after seeing a valid ACK from the client. **Recommendation**: TCP intercept normally does not create a connection for the first SYN, except when there are nailed rules, the packet comes over a VPN tunnel, or the next hop gateway address to reach the client is not resolved. So for the first SYN, this indicates that a connection was created. When TCP intercept receives a RST from server, it is likely that the corresponding port is closed on the server. **System log messages**: None.
tcp-intercept-unexpected	TCP intercept unexpected state	Logic error in the TCP intercept module; this should never happen. **Recommendation**: Indicates memory corruption or some other logic error in the TCP intercept module. **System log messages**: None.
tcpmod-connect-clash	TCP module port collision between client and server	A TCP connect socket clashes with an existing listen connection. This is an internal system error. **Recommendation**: Contact TAC. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
tcpnorm-invalid-syn	TCP invalid SYN	This reason is given for closing a TCP flow when the SYN packet is invalid. **Recommendation**: The SYN packet could be invalid for a number of reasons, such as an invalid checksum or an invalid TCP header. Please use the packet capture feature to understand why the SYN packet is invalid. If you would like to allow these connections, use the **tcp-map** configuration to bypass checks. **System log messages**: 302014
tcpnorm-rexmit-bad	TCP bad retransmission	This reason is given for closing a TCP flow when the **check-retransmission** feature is enabled, and the TCP endpoint sent a retransmission with different data from the original packet. **Recommendation**: The TCP endpoint may be attacking by sending different data in TCP retransmits. Please use the packet capture feature to learn more about the origin of the packet. **System log messages**: 302014
tcpnorm-win-variation	TCP unexpected window size variation	This reason is given for closing a TCP flow when the window size advertised by the TCP endpoint is drastically changed without accepting that much data. **Recommendation**: In order to allow this connection, use the **window-variation** command. **System log messages**: 302014
timeout	Conn-timeout	This counter is incremented when a flow is closed because of the expiration of its inactivity timer. **Recommendation**: None. **System log messages**: 302014, 302016, 302018, 302021
tunnel-pending	Tunnel being brought up or torn down	This counter will increment when the security appliance receives a packet matching an entry in the security policy database (i.e. **crypto map**) but the security association is in the process of being negotiated; its not complete yet. This counter will also increment when the security appliance receives a packet matching an entry in the security policy database but the security association has been or is in the process of being deleted. The difference between this indication and the “"Tunnel has been torn down” indication is that the “Tunnel has been torn down” indication is for established flows. **Recommendation**: This is a normal condition when the IPSec tunnel is in the process of being negotiated or deleted. **System log messages**: None.

Table 25-2 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
tunnel-torn-down	Tunnel has been torn down	This counter will increment when the security appliance receives a packet associated with an established flow whose IPSec security association is in the process of being deleted. **Recommendation**: This is a normal condition when the IPSec tunnel is torn down for any reason. **System log messages**: None
vpn-handle-error	VPN Handle Error	This counter is incremented when the security appliance is unabled to create a VPN handle because the VPN handle already exists. **Recommendation**: It is possible to see this counter increment as part of normal operation. However, if the counter is rapidly incrementing and there is a major malfunction of VPN-based applications, then this may be caused by a software defect. Contact Cisco TAC to investigate the issue further. **System log messages**: None
xlate-removed	Xlate Clear	The flow was removed in response to the **clear xlate** command or **clear local-host** command. **Recommendation**: This is an information counter. **System log messages**: 302014, 302016, 302018, 302021, 305010, 305012, 609002

Examples

The following is sample output from the **show asp drop** command, with the timestamp indicating when the last time the counters were cleared:

```
hostname# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                    3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                   760
  Expired flow (flow-expired)                                     1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                       24
  NAT failed (nat-failed)                                     28739
  NAT reverse path failed (nat-rpf-failed)                    22266
  Inspection failure (inspect-fail)                           19433

Last clearing: 17:02:12 UTC Jan 17 2008 by enable_15
```

Related Commands

Command	Description
capture	Captures packets, including the option to capture packets based on an asp drop code.
clear asp drop	Clears drop statistics for the accelerated security path.
show conn	Shows information about connections.

show asp table arp

To debug the accelerated security path ARP tables, use the **show asp table arp** command in privileged EXEC mode.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

Syntax Description

address *ip_address*	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask *mask*	(Optional) Sets the subnet mask for the IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show arp** command shows the contents of the control plane, while the **show asp table arp** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table arp** command:

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
```

```
::                                      Active   0000.0000.0000 hits 0
0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

Related Commands

Command	Description
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through.

show asp table classify [**hit** | **crypto** | **domain** *domain_name* | **interface** *interface_name*]

Syntax Description

domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See "Usage Guidelines" for a list of domains.
hits	(Optional) Shows classifier entries which have non-zero hits values
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.
crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)	Added the **hits** option, and the timestamp indicating when the last time the asp table counters were cleared.
8.0(2)	A new counter was added to show the number of times a tmatch compilation was aborted. This counter is shown only if the value is greater than 0.

Usage Guidelines

The **show asp table classifier** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Classifier domains include the following:

```
aaa-acct
aaa-auth
```

```
aaa-user
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
priority-q
```

```
punt
punt-l2
punt-root
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

Examples

The following is sample output from the **show asp table classify** command:

```
hostname# show asp table classify

Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

The following is sample output from the **show asp table classify hits** command with a record of the last clearing hits counters:

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command in privileged EXEC mode.

show asp table interfaces

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table interfaces** command:

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
```

```
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show asp table routing

To debug the accelerated security path routing tables, use the **show asp table routing** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

Syntax Description

address *ip_address*	Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter the following: `fe80::2e0:b6ff:fe01:3b7a/128`
input	Shows the entries from the input route table.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask *mask*	For IPv4 addresses, specifies the subnet mask.
output	Shows the entries from the output route table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show asp table routing** command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table routing** command:

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
```

```
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

Related Commands

Command	Description
show route	Shows the routing table in the control plane.

show asp table socket

To debug the accelerated security path socket information, use the **show asp table socket** command in privileged EXEC mode.

show asp table socket

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The **show asp table socket** command lets you debug the accelerated security path socket information.

Examples

This is an example of the the **show asp table socket** command:

```
Protocol  Socket    Local Address             Foreign Address         State
TCP       00012bac  10.86.194.224:23          0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22          0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443         0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443           0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443         0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443               0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443               0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22          171.69.137.139:4190     ESTAB
```

Related Commands

Command	Description
show asp table vpn-context	Debugs the accelerated security path VPN context tables.

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

show asp table vpn-context [**detail**]

Syntax Description

detail	(Optional) Shows additional detail for the VPN context tables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	Added +PRESERVE flag for each context that maintains stateful flows after the tunnel drops.

Usage Guidelines

The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table vpn-context** command:

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

The following is sample output from the **show asp table vpn-context** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag:

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

The following is sample output from the **show asp table vpn-context detail** command:

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

The following is sample output from the **show asp table vpn-context detail** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag.:

```
hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show blocks

To show the packet buffer utilization, use the **show blocks** command in privileged EXEC mode.

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** [**detail**]]

Syntax Description

address *hex*	(Optional) Shows a block corresponding to this address, in hexadecimal.
all	(Optional) Shows all blocks.
assigned	(Optional) Shows blocks that are assigned and in use by an application.
detail	(Optional) Shows a portion (128 bytes) of the first block for each unique queue type.
dump	(Optional) Shows the entire block contents, including the header and packet information. The difference between dump and packet is that dump includes additional information between the header and the packet.
diagnostics	(Optional) Shows block diagnostics.
free	(Optional) Shows blocks that are available for use.
header	(Optional) Shows the header of the block.
old	(Optional) Shows blocks that were assigned more than a minute ago.
packet	(Optional) Shows the header of the block as well as the packet contents.
pool *size*	(Optional) Shows blocks of a specific size.
queue history	(Optional) Shows where blocks are assigned when the security appliance runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
summary	(Optional) Shows detailed information about block usage sorted by the program addresses of applications that allocated blocks in this class, program addresses of applications that released blocks in this class, and the queues to which valid blocks in this class belong.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The **pool summary** option was added.
8.0(2)	The dupb block uses 0 length blocks now instead of 4 byte blocks. An additional line was added for 0 byte blocks.

Usage Guidelines

The **show blocks** command helps you determine if the security appliance is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the security appliance. You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also view this information using SNMP.

The information shown in a security context includes the system-wide information as well as context-specific information about the blocks in use and the high water mark for block usage.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show blocks** command in single mode:

```
hostname# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

Table 25-3 shows each field description.

Table 25-3 show blocks Fields

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type. Examples are shown below.
0	Used by dupb blocks.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules. Also, this sized block can be used normally by code to send packets to drivers, etc.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.

Table 25-3 show blocks Fields (continued)

Field	Description
256	Used for Stateful Failover updates, syslogging, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active security appliance generates and sends packets to the standby security appliance to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby security appliance. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the security appliance is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the security appliance is processing. Syslog messages sent out from the security appliance also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the security appliance configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.
1550	Used to store Ethernet packets for processing through the security appliance. When a packet enters a security appliance interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The security appliance determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the security appliance is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the security appliance attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the security appliance drops the packet.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543). See the description for 1550 for more information about Ethernet packets.
2048	Control or guided frames used for control updates.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the security appliance can dynamically create more when needed, up to a maximum of 8192.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the security appliance was powered up, or since the last clearing of the blocks (with the **clear blocks** command). A zero in the LOW column indicates a previous event where memory was full.
CNT	Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.

The following is sample output from the **show blocks all** command:

```
hostname# show blocks all
Class 0, size 4
```

```
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

Table 25-4 shows each field description.

Table 25-4 show blocks all Fields

Field	Description
Block	The block address.
allocd_by	The program address of the application that last used the block (0 if not used).
freed_by	The program address of the application that last released the block.
data size	The size of the application buffer/packet data that is inside the block.
alloccnt	The number of times this block has been used since the block came into existence.
dup_cnt	The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.
oper	One of the four operations that was last performed on the block: alloc, get, put, or free.
location	The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).

The following is sample output from the **show blocks** command in a context:

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

The following is sample output from the **show blocks queue history** command:

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
```

```
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

The following is sample output from the **show blocks queue history detail** command:

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

The following is sample output from the **show blocks pool summary** command:

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
```

```
         total_count=1531    miss_count=0
Alloc_pc         valid_cnt       invalid_cnt
0x3b0a18         00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b         00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc         valid_cnt       invalid_cnt
0x9a81f3         00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326         00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2         00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue    valid_cnt       invalid_cnt
0x3b0a18         00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b         00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

Table 25-5 shows each field description.

Table 25-5 show blocks pool summary Fields

Field	Description
total_count	The number of blocks for a given class.
miss_count	The number of blocks not reported in the specified category due to technical reasons.
Freed_pc	The program addresses of applications that released blocks in this class.
Alloc_pc	The program addresses of applications that allocated blocks in this class.
Queue	The queues to which valid blocks in this class belong.
valid_cnt	The number of blocks that are currently allocated.
invalid_cnt	The number of blocks that are not currently allocated.
Invalid Bad qtype	Either this queue has been freed and the contents are invalid or this queue was never initialized.
Valid tcp_usr_conn_inp	The queue is valid.

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
clear blocks	Clears the system buffer statistics.
show conn	Shows active connections.

show bootvar

To show the boot file and configuration properties, use the **show boot** command in privileged EXEC mode.

show bootvar

Syntax Description

show bootvar	The system boot properties.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. Set these variables with the **boot system** command, and **boot config** command, respectively.

Examples

The following example, the BOOT variable contains disk0:/f1_image, which is the image booted when the system reloads. The current value of BOOT is disk0:/f1_image; disk0:/f1_backupimage. This meansboot variable has been modified with the boot system command, but the running configuration has notbeen saved with the **write memory** command. When the running config is saved, the BOOT variable and current BOOT variable will both be disk0:/f1_image; disk0:/f1_backupimage. Assuming the running configuration is saved the boot loader will attempt to load the contents of the BOOT variable, starting with disk0:/f1image, but if that is not present or invalid, it will attempt to boot disk0:1/f1_backupimage.

The CONFIG_FILE variable points to the system startup configuration. In this example it is not set, so the startup configuration file is the default specified with the **boot config** command. The current CONFIG_FILE variable may be modified with the **boot config** command and saved with the **write memory** command.

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

```
hostname#
```

Related Commands

Command	Description
boot	Specifies the configuration file or image file used at startup.

show capture

To display the capture configuration when no options are specified, use the **show capture** command.

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

Syntax Description

capture_name	(Optional) Name of the packet capture.
access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count *number*	(Optional) Displays the number of packets specified data.
decode	This option is useful when a capture of type isakmp is applied to an interface. All isakmp data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link transport.
packet-number *number*	Starts the display at the specified packet number.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you specify the *capture_name*, then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In Table 25-6, the bracketed output is displayed when you specify the **detail** keyword.

Table 25-6 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

Examples

This example shows how to display the capture configuration:

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.

show chardrop

To display the count of characters dropped from the serial console, use the **show chardrop** command in privileged EXEC mode.

show chardrop

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show chardrop** command:

```
hostname# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show checkheaps

To show the checkheaps statistics, use the **show checkheaps** command in privileged EXEC mode. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

show checkheaps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show checkheaps** command:

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

Related Commands

Command	Description
checkheaps	Sets the checkheap verification intervals.

show checksum

To display the configuration checksum, use the **show checksum** command in privileged EXEC mode.

show checksum

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the security appliance.

Usage Guidelines

The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in Flash memory.

If a dot (".") appears before the checksum in the **show config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the security appliance Flash partition). The "." shows that the security appliance is preoccupied with the operation but is not "hung up." This message is similar to a "system processing, please wait" message.

Examples

This example shows how to display the configuration or the checksum:

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command in privileged EXEC mode.

show chunkstat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to display the chunk statistics:

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

show class

To show the contexts assigned to a class, use the **show class** command in privileged EXEC mode.

show class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To show the default class, enter **default** for the name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show class default** command:

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

Related Commands

Command	Description
class	Configures a resource class.
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.

show clock

To view the time on the security appliance, use the **show clock** command in user EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP or user configuration) and the current summer-time setting (if any).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show clock** command:

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

The following is sample output from the **show clock detail** command:

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show ntp status	Shows the status of the NTP association.

show compression svc

To view compression statistics for SVC connections on the security appliance, use the **show compression svc** command from privileged EXEC mode:

show compression svc

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example shows the output of the **show compression svc** command:

```
hostname# show compression svc
Compression SVC Sessions                        1
Compressed Frames                          249756
Compressed Data In (bytes)                0048042
Compressed Data Out (bytes)               4859704
Expanded Frames                                 1
Compression Errors                              0
Compression Resets                              0
Compression Output Buf Too Small                0
Compression Ratio                            2.06
Decompressed Frames                        876687
Decompressed Data In                     279300233
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of http data over an SVC connection for a specific group or user.

show configuration

To display the configuration that is saved in flash memory on the security appliance, use the **show configuration** command in privileged EXEC mode.

show configuration

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was modified.

Usage Guidelines

The **show configuration** command displays the saved configuration in flash memory on the security appliance. Unlike the **show running-config** command, the **show configuration** command does not use many CPU resources to run.

To display the active configuration in memory (including saved configuration changes) on the security appliance, use the **show running-config** command.

Examples

This example shows how to display the configuration that is saved in flash memory on the security appliance:

```
hostname# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
```

```
 nameif dmz
 security-level 50
 ip address 40.0.0.5 255.0.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 40.0.0.0 255.0.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
```

```
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

Related Commands

Command	Description
configure	Configures the security appliance from the terminal.

show conn

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}]
[**address** *src_ip*[-*src_ip*] [**netmask** *mask*]] [**port** *src_port*[-*src_port*]]
[**address** *dest_ip*[-*dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[-*dest_port*]]]

Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
detail	(Optional) Displays connections in detail, including translation type and interface information.
long	(Optional) Displays connections in long format.
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol {tcp | udp}	(Optional) Specifies the connection protocol, **tcp** or **udp**.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
state *state_type*	(Optional) Specifies the connection state type. See Table 25-7 for a list of the keywords available for connection state types.

Defaults

All through connections are shown by default. You need to use the **all** keyword to also view management connections to the device.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	The syntax was simplified to use source and destination concepts instead of “local” and “foreign.” In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like **foreign** and **fport** to determine the destination address and port.

Usage Guidelines

The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the **show conn all** command to see the entire table of connections.

Note When the security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

The connection types that you can specify using the **show conn state** command are defined in Table 25-7. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 25-7 Connection State Types

Keyword	Connection Type Displayed
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.
rpc	RPC connections.

Table 25-7 Connection State Types (continued)

Keyword	Connection Type Displayed
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.
vpn_orphan	Orphaned VPN tunneled flows.

When you use the **detail** option, the system displays information about the translation type and interface information using the connection flags defined in Table 25-8.

Table 25-8 Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group[1]
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data
k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection
q	SQL*Net data
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection

Table 25-8 Connection Flags (continued)

Flag	Description
R	UDP RPC[2]
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection[3]
T	SIP connection[4]
U	up
V	VPN orphan
W	WAAS
X	Inspected by the service module, such as a CSC SSM.

1. The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
2. Because each row of **show conn** command output represents one connection (TCP or UDP), there will be only one R flag per row.
3. For UDP connections, the value t indicates that it will timeout after one minute.
4. For UDP connections, the value T indicates that the connection will timeout according to the value specified using the **timeout sip** command.

Note For connections using a DNS server, the source port of the connection may be replaced by the *IP address of DNS server* in the **show conn** command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, when you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

Note When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The **show conn** command output shows these orphaned flows with the **V** flag.

Examples

When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

```
hostname# show conn state up,rpc,h323,sip
```

The following is sample output from the **show conn count** command:

```
hostname# show conn count
54 in use, 123 most used
```

The following is sample output from the **show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The “U”, “I”, and “O” flags denote that the connection is active and has received inbound and outbound data.

```
hostname# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

The following is sample output from the **show conn** command, whcih includes the “X” flag to indicate that the connection is being scanned by the SSM.

```
hostname# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

The following is sample output from the **show conn detail** command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
hostname# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
```

```
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

The following is sample output from the **show conn** command when an orphan flow exists, as indicated by the **V** flag:

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

To limit the report to those connections that have orphan flows, add the **vpn_orphan** option to the **show conn state** command, as in the following example:

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

Related Commands

Commands	Description
clear conn	Clears connections.
inspect ctiqbe	Enables CTIQBE application inspection.
inspect h323	Enables H.323 application inspection.
inspect mgcp	Enables MGCP application inspection.
inspect sip	Removes Java applets from HTTP traffic.
inspect skinny	Enables SCCP application inspection.

show console-output

To display the currently captured console output, use the **show console-output** command in privileged EXEC mode.

show console-output

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows the message that displays when there is no console output:

```
hostname# show console-output
Sorry, there are no messages to display
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
console timeout	Sets the idle timeout for a console connection to the security appliance.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

show context

To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.

show context [*name* | **detail** | **count**]

Syntax Description

count	(Optional) Shows the number of contexts configured.
detail	(Optional) Shows additional detail about the context(s) including the running state and information for internal use.
name	(Optional) Sets the context name. If you do not specify a name, the security appliance displays all contexts. Within a context, you can only enter the current context name.

Defaults

In the system execution space, the security appliance displays all contexts if you do not specify a name.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	Information about assigned IPS virtual sensors was added.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Table 25-9 shows each field description.

Table 25-9 show context Fields

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Interfaces	The interfaces assigned to the context.
URL	The URL from which the security appliance loads the context configuration.

The following is sample output from the **show context detail** command in the system execution space:

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Table 25-10 shows each field description.

Table 25-10 Context States

Field	Description
Context	The context name. The null context information is for internal use only. The system context represents the system execution space.
State Message:	The context state. See the possible messages below.
Has been created, but initial ACL rules not complete	The security appliance parsed the configuration but has not yet downloaded the default ACLs to establish the default security policy. The default security policy applies to all contexts initially, and includes disallowing traffic from lower security levels to higher security levels, enabling application inspection, and other parameters. This security policy ensures that no traffic can pass through the security appliance after the configuration is parsed but before the configuration ACLs are compiled. You are unlikely to see this state because the configuration ACLs are compiled very quickly.
Has been created, but not initialized	You entered the **context** *name* command, but have not yet entered the **config-url** command.
Has been created, but the config hasn't been parsed	The default ACLs were downloaded, but the security appliance has not parsed the configuration. This state might exist because the configuration download might have failed because of network connectivity issues, or you have not yet entered the **config-url** command. To reload the configuration, from within the context, enter **copy startup-config running-config**. From the system, reenter the **config-url** command. Alternatively, you can start configuring the blank running configuration.
Is a system resource	This state applies only to the system execution space and to the null context. The null context is used by the system, and the information is for internal use only.
Is a zombie	You deleted the context using the **no context** or **clear context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Is active	This context is currently running and can pass traffic according to the context configuration security policy.
Is ADMIN and active	This context is the admin context and is currently running.
Was a former ADMIN, but is now a zombie	You deleted the admin context using the **clear configure context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Real Interfaces	The interfaces assigned to the context. If you mapped the interface IDs in the **allocate-interface** command, this display shows the real name of the interface.
Mapped Interfaces	If you mapped the interface IDs in the **allocate-interface** command, this display shows the mapped names. If you did not map the interfaces, the display lists the real names again.

Table 25-10 Context States (continued)

Field	Description
Real IPS Sensors	The IPS virtual sensors assigned to the context if you have an AIP SSM installed. If you mapped the sensor names in the **allocate-ips** command, this display shows the real name of the sensor.
Mapped IPS Sensors	If you mapped the sensor names in the **allocate-ips** command, this display shows the mapped names. If you did not map the sensor names, the display lists the real names again.
Flag	For internal use only.
ID	An internal ID for this context.

The following is sample output from the **show context count** command:

```
hostname# show context count
Total active contexts: 2
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

show controller

To view controller-specific information of all interfaces present, use the **show controller** command in privileged EXEC mode.

show controller [*physical_interface*] [**detail**]

Syntax Description

detail	(Optional) Shows additional detail about the controller.
physical_interface	(Optional) Identifies the interface ID.

Defaults

If you do not identify a switch port, this command shows information for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	This command now applies to all platforms, and not just the ASA 5505. The **detail** keyword was added.

Usage Guidelines

This command helps Cisco TAC gather useful debug information about the controller when investigating internal and customer found defects. The actual output depends on the model and Ethernet controller.

Examples

The following is sample output from the **show controller** command:

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
```

```
        Identifier:    0x0952  Port Ctrl:     0x0074
        Port Ctrl-1:   0x0000  Vlan Map:      0x077f
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0080
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000

    Global Registers:
        Control:       0x0482

----------------------------------------------------------------------
Number of VLANs: 1
----------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
----------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
----------------------------------------------------------------------

Ethernet0/1:
   Marvell 88E6095 revision 2, switch port 6
     PHY Register:
        Control:       0x3000  Status:        0x7849
        Identifier1:   0x0141  Identifier2:   0x0c85
        Auto Neg:      0x01e1  LP Ability:    0x0000
        Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x0130
        PHY Status:    0x0040  PHY Intr En:   0x0400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
        Status:        0x0007  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07bf
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0040
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/2:
   Marvell 88E6095 revision 2, switch port 5
     PHY Register:
        Control:       0x3000  Status:        0x786d
        Identifier1:   0x0141  Identifier2:   0x0c85
        Auto Neg:      0x01e1  LP Ability:    0x41e1
        Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
        PHY Status:    0x6c00  PHY Intr En:   0x0400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
        Status:        0x0d07  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07df
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0020
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/3:
   Marvell 88E6095 revision 2, switch port 4
     PHY Register:
```

```
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07ef
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0010
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/4:
   Marvell 88E6095 revision 2, switch port 3
     PHY Register:
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07f7
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0008
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/5:
   Marvell 88E6095 revision 2, switch port 2
     PHY Register:
          Control:       0x3000  Status:        0x786d
          Identifier1:   0x0141  Identifier2:   0x0c85
          Auto Neg:      0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:    0x6c00  PHY Intr En:   0x0400
          Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
          Led select:    0x1a34
          Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
          Status:        0x0d07  PCS Ctrl:      0x0003
          Identifier:    0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:   0x0000  Vlan Map:      0x07fb
          VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:   0x0004
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
          Control:       0x3000  Status:        0x7849
```

```
        Identifier1:   0x0141  Identifier2:   0x0c85
        Auto Neg:      0x01e1  LP Ability:    0x0000
        Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
        PHY Status:    0x0040  PHY Intr En:   0x8400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
      Port Registers:
        Status:        0x0007  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0002
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Ethernet0/7:
   Marvell 88E6095 revision 2, switch port 0
     PHY Register:
        Control:       0x3000  Status:        0x7849
        Identifier1:   0x0141  Identifier2:   0x0c85
        Auto Neg:      0x01e1  LP Ability:    0x0000
        Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
        PHY Status:    0x0040  PHY Intr En:   0x8400
        Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
        Status:        0x0007  PCS Ctrl:      0x0003
        Identifier:    0x0952  Port Ctrl:     0x0077
        Port Ctrl-1:   0x0000  Vlan Map:      0x07fe
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0001
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
```

```
    PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
    OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
    TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Internal-Data0/0:
    Y88ACS06 Register settings:
     rap                           0xe0004000 = 0x00000000
     ctrl_status                   0xe0004004 = 0x5501064a
     irq_src                       0xe0004008 = 0x00000000
     irq_msk                       0xe000400c = 0x00000000
     irq_hw_err_src                0xe0004010 = 0x00000000
     irq_hw_err_msk                0xe0004014 = 0x00001000
     bmu_cs_rxq                    0xe0004060 = 0x002aaa80
     bmu_cs_stxq                   0xe0004068 = 0x01155540
     bmu_cs_atxq                   0xe000406c = 0x012aaa80

    Bank 2: MAC address registers:
     mac_addr1_lo                  0xe0004100 = 0x00000000
     mac_addr1_hi                  0xe0004104 = 0x00000000
     mac_addr2_lo                  0xe0004108 = 0x00000000
     mac_addr2_hi                  0xe000410c = 0x00000000
     mac_addr3_lo                  0xe0004110 = 0x00000000
     mac_addr3_hi                  0xe0004114 = 0x00000000
     chip_info                     0xe0004118 = 0xb0110000
     eprom                         0xe000411c = 0x00000000
     flash_addr_reg                0xe0004120 = 0x0001fffe
     flash_data_port               0xe0004124 = 0x000000ff
     loader                        0xe0004128 = 0x00000400
     timer_init_val                0xe0004130 = 0x00000000
     timer_val                     0xe0004134 = 0x00000000
     timer_ctrl                    0xe0004138 = 0x00000202
     irq_mod_timer_init_val        0xe0004140 = 0x00000000
     irq_mod_timer                 0xe0004144 = 0x00000000
     irq_mod_timer_ctrl            0xe0004148 = 0x00000202
     irq_mod_msk                   0xe000414c = 0x00000000
     irq_hw_err_mod_mask           0xe0004150 = 0x00000000
     tst_ctrl                      0xe0004158 = 0x00000001
     gp_io                         0xe000415c = 0x0000000f
     i2c_ctrl                      0xe0004160 = 0x00000000
     i2c_data                      0xe0004164 = 0x00000000
     i2c_irq                       0xe0004168 = 0x00000000
     i2c_sw                        0xe000416c = 0x00000003

    RAM Random Registers:
     ram_addr                      0xe0004180 = 0x00000000
     ram_data_port_lo              0xe0004184 = 0x00000000
     ram_data_port_hi              0xe0004188 = 0x00000000

    Ram Interface Registers:
     ram_if_to_lo                  0xe0004190 = 0x24242424
     ram_if_to_hi                  0xe0004194 = 0x00002424
     ram_if_timeout_val            0xe000419c = 0x00000000
     ram_if_ctrl                   0xe00041a0 = 0x000a0002

    Transmit Arbiter MAC:
     tx_arb_iti_init               0xe0004200 = 0x00000000
     tx_arb_iti_val                0xe0004204 = 0x00000000
     tx_arb_lim_init               0xe0004208 = 0x00000000
     tx_arb_lim_val                0xe000420c = 0x00000000
     tx_arb_ctrl_tst_status        0xe0004210 = 0x00001256

    Bank 8: Receive queue registers:
     rx_qregs.buf_ctrl             0xe0004400 = 0xc8550800
     rx_qregs.next_desc_addr_lo    0xe0004404 = 0x016d4020
```

```
 rx_qregs.buf_addr_lo          0xe0004408 = 0x019acd00
 rx_qregs.buf_addr_hi          0xe000440c = 0x00000000
 rx_qregs.frame_sw             0xe0004410 = 0x00000000
 rx_qregs.time_stamp           0xe0004414 = 0x00000000
 rx_qregs.tcp_csum             0xe0004418 = 0x00000000
 rx_qregs.tcp_csum_start       0xe000441c = 0x00000000
 rx_qregs.desc_addr_lo         0xe0004420 = 0x016d4000
 rx_qregs.desc_addr_hi         0xe0004424 = 0x00000000
 rx_qregs.addr_cntr_lo         0xe0004428 = 0x016d4020
 rx_qregs.addr_cntr_hi         0xe000442c = 0x00000000
 rx_qregs.byte_cntr            0xe0004430 = 0x00000000
 rx_qregs.bmu_cs               0xe0004434 = 0x002aaa80
 rx_qregs.flag                 0xe0004438 = 0x00000600
 rx_qregs.tst1                 0xe000443c = 0xd2020202
 rx_qregs.tst2                 0xe0004440 = 0x00000050
 rx_qregs.tst3                 0xe0004444 = 0x00000000

Bank 12: Synchronous transmit queue registers:
 stx_qregs.buf_ctrl            0xe0004600 = 0x00000000
 stx_qregs.next_desc_addr_lo   0xe0004604 = 0x00000000
 stx_qregs.buf_addr_lo         0xe0004608 = 0x00000000
 stx_qregs.buf_addr_hi         0xe000460c = 0x00000000
 stx_qregs.frame_sw            0xe0004610 = 0x00000000
 stx_qregs.time_stamp          0xe0004614 = 0x00000000
 stx_qregs.tcp_csum            0xe0004618 = 0x00000000
 stx_qregs.tcp_csum_start      0xe000461c = 0x00000000
 stx_qregs.desc_addr_lo        0xe0004620 = 0x00000000
 stx_qregs.desc_addr_hi        0xe0004624 = 0x00000000
 stx_qregs.addr_cntr_lo        0xe0004628 = 0x00000000
 stx_qregs.addr_cntr_hi        0xe000462c = 0x00000000
 stx_qregs.byte_cntr           0xe0004630 = 0x00000000
 stx_qregs.bmu_cs              0xe0004634 = 0x01155540
 stx_qregs.flag                0xe0004638 = 0x0a000600
 stx_qregs.tst1                0xe000463c = 0x02020202
 stx_qregs.tst2                0xe0004640 = 0x00000050
 stx_qregs.tst3                0xe0004644 = 0x00000000

Bank 13: Asynchronous transmit queue registers:
 atx_qregs.buf_ctrl            0xe0004680 = 0x00000000
 atx_qregs.next_desc_addr_lo   0xe0004684 = 0x00000000
 atx_qregs.buf_addr_lo         0xe0004688 = 0x00000000
 atx_qregs.buf_addr_hi         0xe000468c = 0x00000000
 atx_qregs.frame_sw            0xe0004690 = 0x00000000
 atx_qregs.time_stamp          0xe0004694 = 0x00000000
 atx_qregs.tcp_csum            0xe0004698 = 0x00000000
 atx_qregs.tcp_csum_start      0xe000469c = 0x00000000
 atx_qregs.desc_addr_lo        0xe00046a0 = 0x016d9000
 atx_qregs.desc_addr_hi        0xe00046a4 = 0x00000000
 atx_qregs.addr_cntr_lo        0xe00046a8 = 0x016d901c
 atx_qregs.addr_cntr_hi        0xe00046ac = 0x00000000
 atx_qregs.byte_cntr           0xe00046b0 = 0x00000000
 atx_qregs.bmu_cs              0xe00046b4 = 0x012aaa80
 atx_qregs.flag                0xe00046b8 = 0x0a000600
 atx_qregs.tst1                0xe00046bc = 0x02020202
 atx_qregs.tst2                0xe00046c0 = 0x00000050
 atx_qregs.tst3                0xe00046c4 = 0x00000000

Bank 16: Receive RAM buffer registers:
 rx_ram_buf_regs.start_addr    0xe0004800 = 0x00000000
 rx_ram_buf_regs.end_addr      0xe0004804 = 0x000017ff
 rx_ram_buf_regs.wr_ptr        0xe0004808 = 0x00000000
 rx_ram_buf_regs.rd_ptr        0xe000480c = 0x00000000
 rx_ram_buf_regs.up_thres_pp   0xe0004810 = 0x00001400
 rx_ram_buf_regs.lo_thres_pp   0xe0004814 = 0x00001000
```

```
 rx_ram_buf_regs.up_thres_hp   0xe0004818 = 0x00000000
 rx_ram_buf_regs.lo_thres_hp   0xe000481c = 0x00000000
 rx_ram_buf_regs.pak_cnt       0xe0004820 = 0x00000000
 rx_ram_buf_regs.level         0xe0004824 = 0x00000000
 rx_ram_buf_regs.ctrl          0xe0004828 = 0x0002222a

Bank 20: Synchronous transmit RAM buffer registers:
 stx_ram_buf_regs.start_addr   0xe0004a00 = 0x00000000
 stx_ram_buf_regs.end_addr     0xe0004a04 = 0x00000000
 stx_ram_buf_regs.wr_ptr       0xe0004a08 = 0x00000000
 stx_ram_buf_regs.rd_ptr       0xe0004a0c = 0x00000000
 stx_ram_buf_regs.pak_cnt      0xe0004a20 = 0x00000000
 stx_ram_buf_regs.level        0xe0004a24 = 0x00000000
 stx_ram_buf_regs.ctrl         0xe0004a28 = 0x00022215

Bank 21: Asynchronous transmit RAM buffer registers:
 atx_ram_buf_regs.start_addr   0xe0004a80 = 0x00001800
 atx_ram_buf_regs.end_addr     0xe0004a84 = 0x00002fff
 atx_ram_buf_regs.wr_ptr       0xe0004a88 = 0x00001800
 atx_ram_buf_regs.rd_ptr       0xe0004a8c = 0x00001800
 atx_ram_buf_regs.up_thres_pp  0xe0004a90 = 0x00000000
 atx_ram_buf_regs.lo_thres_pp  0xe0004a94 = 0x00000000
 atx_ram_buf_regs.up_thres_hp  0xe0004a98 = 0x00000000
 atx_ram_buf_regs.lo_thres_hp  0xe0004a9c = 0x00000000
 atx_ram_buf_regs.pak_cnt      0xe0004aa0 = 0x00000000
 atx_ram_buf_regs.level        0xe0004aa4 = 0x00000000
 atx_ram_buf_regs.ctrl         0xe0004aa8 = 0x0002222a

Bank 24: Receive GMAC FIFO registers:
 rx_gmfifo_regs.end_addr       0xe0004c40 = 0x0000007f
 rx_gmfifo_regs.thr            0xe0004c44 = 0x00000070
 rx_gmfifo_regs.ctrl           0xe0004c48 = 0x0000224a

Bank 26: Transmit GMAC FIFO registers:
 tx_gmfifo_regs.end_addr       0xe0004d40 = 0x0000007f
 tx_gmfifo_regs.thr            0xe0004d44 = 0x00000010
 tx_gmfifo_regs.ctrl           0xe0004d48 = 0x0002220a
 tx_gmfifo_regs.wr_ptr         0xe0004d60 = 0x00000000
 tx_gmfifo_regs.wr_shdw_ptr    0xe0004d64 = 0x00000000
 tx_gmfifo_regs.wr_level       0xe0004d68 = 0x00000000
 tx_gmfifo_regs.rd_ptr         0xe0004d70 = 0x00000000
 tx_gmfifo_regs.restart_ptr    0xe0004d74 = 0x00000000
 tx_gmfifo_regs.rd_level       0xe0004d78 = 0x00000000

Descriptor poll timer registers:
 dpt_init_val                  0xe0004e00 = 0x00000000
 dpt_val                       0xe0004e04 = 0x00000000
 dpt_ctrl                      0xe0004e08 = 0x00020001

Timestamp timer register:
 ts_timer_val                  0xe0004e14 = 0x00000000
 ts_timer_ctrl                 0xe0004e18 = 0x00000202

GMAC and GPHY control registers:
 gmac_ctrl                     0xe0004f00 = 0x00000056
 gphy_ctrl                     0xe0004f04 = 0x0b7de002
 gmac_irq_src                  0xe0004f08 = 0x00000000
 gmac_irq_msk                  0xe0004f0c = 0x0000003a
 gmac_link_ctrl                0xe0004f10 = 0x00000002

Wake on LAN control registers:
 wol_ctrl                      0xe0004f20 = 0x00000555
 wol_mac_addr_lo               0xe0004f24 = 0x00000000
 wol_mac_addr_hi               0xe0004f28 = 0x00000000
```

```
    wol_patt_rd_ptr               0xe0004f2c = 0x00000000
    wol_patt_len_lo               0xe0004f30 = 0x3b3b3b3b
    wol_patt_len_hi               0xe0004f34 = 0x003b3b3b
    wol_patt_cnt_lo               0xe0004f38 = 0x00000000
    wol_patt_cnt_hi               0xe0004f3c = 0x00000000

   Bank 80 (0x50): GMAC registers:
    gmac_gpsr                     0xe0006800 = 0x0000f014
    gmac_gpcr                     0xe0006804 = 0x000038ff
    gmac_tx_ctrl                  0xe0006808 = 0x00001c00
    gmac_rx_ctrl                  0xe000680c = 0x0000a000
    gmac_tx_fctrl                 0xe0006810 = 0x0000ffff
    gmac_tx_parm                  0xe0006814 = 0x0000c000
    gmac_smod                     0xe0006818 = 0x00002306
    gmac_sa1_lo                   0xe000681c = 0x0000d000
    gmac_sa1_md                   0xe0006820 = 0x0000ff2b
    gmac_sa1_hi                   0xe0006824 = 0x00009f44
    gmac_sa2_lo                   0xe0006828 = 0x0000d000
    gmac_sa2_md                   0xe000682c = 0x0000ff2b
    gmac_sa2_hi                   0xe0006830 = 0x00009f44
    gmac_mcast_addr_hash1         0xe0006834 = 0x00000000
    gmac_mcast_addr_hash2         0xe0006838 = 0x00000000
    gmac_mcast_addr_hash3         0xe000683c = 0x00000000
    gmac_mcast_addr_hash4         0xe0006840 = 0x00000000
    gmac_tx_irq_src               0xe0006844 = 0x00000000
    gmac_rx_irq_src               0xe0006848 = 0x00000000
    gmac_tr_irq_src               0xe000684c = 0x00000000
    gmac_tx_irq_msk               0xe0006850 = 0x00000000
    gmac_rx_irq_msk               0xe0006854 = 0x00000000
    gmac_tr_irq_msk               0xe0006858 = 0x00000000

Internal-Data0/1:
   Marvell 88E6095 revision 2, switch port 8
     Port Registers:
         Status:        0x0e84  PCS Ctrl:      0xc13e
         Identifier:    0x0952  Port Ctrl:     0x0177
         Port Ctrl-1:   0x0000  Vlan Map:      0x06ff
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0100
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
```

The following is sample output from the **show controller detail** command:

```
hostname# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
```

```
    RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
    RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
    RX Descriptor 0 Length:     0xf8262808 = 0x00001000
    RX Descriptor 0 Head:       0xf8262810 = 0x00000000
    RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
    RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
    RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
    RX Descriptor 1 Length:     0xf8260140 = 0x00000000
    RX Descriptor 1 Head:       0xf8260148 = 0x00000000
    RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

TX Descriptor Registers:
    TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
    TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
    TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
    TX Descriptor 0 Length:     0xf8263808 = 0x00001000
    TX Descriptor 0 Head:       0xf8263810 = 0x00000000
    TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

RX Address Array:
    Ethernet Address 0:         0012.d948.ef58
    Ethernet Address 1:         Not Valid!
    Ethernet Address 2:         Not Valid!
    Ethernet Address 3:         Not Valid!
    Ethernet Address 4:         Not Valid!
    Ethernet Address 5:         Not Valid!
    Ethernet Address 6:         Not Valid!
    Ethernet Address 7:         Not Valid!
    Ethernet Address 8:         Not Valid!
    Ethernet Address 9:         Not Valid!
    Ethernet Address a:         Not Valid!
    Ethernet Address b:         Not Valid!
    Ethernet Address c:         Not Valid!
    Ethernet Address d:         Not Valid!
    Ethernet Address e:         Not Valid!
    Ethernet Address f:         Not Valid!

PHY Registers:
    Phy Control:                0x1140
    Phy Status:                 0x7969
    Phy ID 1:                   0x0141
    Phy ID 2:                   0x0c25
    Phy Autoneg Advertise:      0x01e1
    Phy Link Partner Ability:   0x41e1
    Phy Autoneg Expansion:      0x0007
    Phy Next Page TX:           0x2801
    Phy Link Partnr Next Page:  0x0000
    Phy 1000T Control:          0x0200
    Phy 1000T Status:           0x4000
    Phy Extended Status:        0x3000

Detailed Output - RX Descriptor Ring:

rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

........
```

Related Commands

Command	Description
show interface	Shows the interface statistics.
show tech-support	Shows information so Cisco TAC can diagnose problems.

show counters

To display the protocol stack counters, use the **show counters** command in privileged EXEC mode.

show counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

Syntax Description

all	Displays the filter details.
context *context-name*	Specifies the context name.
:*counter_name*	Specifies a counter by name.
detail	Displays additional counters information.
protocol *protocol_name*	Displays the counters for the specified protocol.
summary	Displays a counter summary.
threshold *N*	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

show counters summary detail threshold 1

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to display all counters:

```
hostname# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

hostname# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
```

The following example shows how to display a summary of counters:

```
hostname# show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

The following example shows how to display counters for a context:

```
hostname# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

Related Commands

Command	Description
clear counters	Clears the protocol stack counters.

show cpu

To display the CPU utilization information, use the **show cpu usage** command in privileged EXEC mode.

show cpu [**usage**]

From the system configuration in multiple context mode:

show cpu [**usage**] [**context** {**all** | *context_name*}]

Syntax Description

all	Specifies that the display show all contexts.
context	Specifies that the display show a context.
context_name	Specifies the name of the context to display.
usage	(Optional) Displays the CPU usage.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The cpu usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the **show cpu** command to find process related loads (that is, activity on behalf of items listed by the output of the **show process** command in both single mode and from the system configuration in multiple context mode).

Further, you can request, when in multiple context mode, a breakdown of the process related load to CPU consumed by any configured contexts by changing to each context and entering the **show cpu** command or by entering the **show cpu context** variant of this command.

While process related load is rounded to the nearest whole number, context related loads include one additional decimal digit of precision. For example, entering **show cpu** from the system context produces a different number than from entering the **show cpu context system** command. The former is an approximate summary of everything in **show cpu context all**, and the latter is only a portion of that summary.

Examples

The following example shows how to display the CPU utilization:

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

This example shows how to display the CPU utilization for the system context in multiple mode:

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

The following shows how to display the CPU utilization for all contexts:

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

This example shows how to display the CPU utilization for a context named “one”:

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

show crashinfo

To display the contents of the crash file stored in Flash memory, enter the **show crashinfo** command in privileged EXEC mode.

show crashinfo [**save**]

Syntax Description

save	(Optional) Displays if the security appliance is configured to save crash information to Flash memory or not.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the crash file is from a test crash (generated from the **crashinfo test** command), the first string of the crash file is "`: Saved_Test_Crash`" and the last string is "`: End_Test_Crash`". If the crash file is from a real crash, the first string of the crash file is "`: Saved_Crash`" and the last string is "`: End_Crash`". (This includes crashes from use of the **crashinfo force page-fault** or **crashinfo force watchdog** commands).

If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo** command displays an error message.

Examples

The following example shows how to display the current crash information configuration:

```
hostname# show crashinfo save
crashinfo save enable
```

The following example shows the output for a crash file test. (However, this test does not actually crash the security appliance. It provides a simulated example file.)

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
```

```
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
```

```
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
```

```
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
```

```
This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
```

```
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8           0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8           0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18           0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718           0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8           0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8           0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8           0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8           0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600           0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8           0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8           0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8           0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8           0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90           0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8           0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920           0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8           0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30           0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368           0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674           0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4           0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534        2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0        4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8           0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360           0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0           0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20           0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8           0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40   508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8           0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0           0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198           0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174           0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150           0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850           0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c           0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108           0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4           0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0           0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534           0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c           0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078           0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054           0 00f51d64 3832/4096 tcp_thread/2
```

```
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

Related Commands

Command	Description
clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces a crash of the security appliance.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.

show crashinfo console

To display the configuration setting of the **crashinfo console** command, enter the **show crashinfo console** command.

show crashinfo console

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

Compliance with FIPS 140-2 prohibits the distribution of Critical Secu rity Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

Examples

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.

Command	Description
fips self-test poweron	Executes power-on self-tests.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the **show crypto accelerator statistics** command in global configuration or privileged EXEC mode.

show crypto accelerator statistics

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays global crypto accelerator statistics:

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
```

```
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
```

```
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto ca certificates

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

show crypto ca certificates [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CA certificate for a trustpoint named tp1:

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
```

```
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ca crls

To display all cached CRLs or to display all CRLs cached for a specified trustpoint, use the **show crypto ca crls** command in global configuration or privileged EXEC mode.

show crypto ca crls [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CRL for a trustpoint named tp1:

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ca server

To display the status of the local Certificate Authority (CA) configuration on the security appliance, use the **show crypto ca server** command.

show crypto ca server

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example displays the status of all configuration data for the local CA server:

```
hostname# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
    Current primary storage dir: nvram:
hostname#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
debug crypto ca server	Shows debug messages when you configure the local CA server.

Command	Description
show crypto ca server certificate	Displays the certificate of the local CA in base64 format.
show crypto ca server crl	Displays the lifetime of the local CA CRL.

show crypto ca server cert-db

To display all or a subset of local Certificate Authority (CA) server certificates including those issued to a specific user, use the **show crypto ca server cert-db** command.

show crypto ca server cert-db [user *username* **| allowed | enrolled | expired | on-hold]**
[serial *certificate-serial-number*]

EW Note???: Per AP, this command will change; currently undefined. Bug #CSCsg36072. Cert # OK now.

Syntax Description

allowed	Specifies that users who are allowed to enroll display, regardless of the status of their certificate.
enrolled	Specifies that users with valid certificates display.
expired	Specifies that users holding expired certificates display.
on-hold	Specifies that users who have not enrolled yet display.
serial *certificate-serial-number*	Specifies the serial number of a specific certificate that is to be displayed. Enter the serial number in hexadecimal format.
user *username*	Specifies the certificate owner. The username can be a simple username or e-mail address.

Defaults

By default, if no username or certificate serial number are specified, the entire database of issued certificates displays.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **show crypto ca server cert-db** command displays a list of the user certificates issued by the local CA server. You can display a subset of the certificate database by specifying a specific user name with one or more of the optional certificate-type keywords, and/or with an optional certificate serial number.

If you specify a user name without a keyword or a serial number, all of the certificates issued for that user display. For each user, the display shows the user name, the *renewal allowed till* field, the *number of times the user is notified* count, and the *PKCS12 file stored till* value before listing each certificate issued for that user.

Each certificate displays with the certificate serial number, the issued and expired dates, and the certificate status (Revoked/Not Revoked).

Examples

The following example requests display of all of the certificates issued for Janedoe by the CA server:

```
hostname# show crypto ca server cert-db user janedoe
```

The following example requests the display of all the certificates issued by the local CA server with a serial number of 0x100 and above:

```
hostname# show crypto ca server cert-db serial 1oo
```

The following example requests display of all of the certificates issued by the local CA server:

```
hostname# show crypto ca server cert-db
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in both the certificate database and Certificate Revocation List (CRL).
lifetime crl	Specifies the lifetime of the certificate revocation list.

show crypto ca server certificate

To display the certificate for the local Certificate Authority (CA) server in base64 format, use the **show crypto ca server certificate** command.

show crypto ca server certificate

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **show crypto ca server certificate** command displays the local CA server certificate in base64 format. This allows you to cut and paste a certificate while exporting it to other devices that need to trust the local CA server.

Examples

The following example displays the server certificate for the local CA server:

```
hostname# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

hostname#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate and issued certificates.
show crypto ca server	Displays the local CA configuration in ASCII text format.

show crypto ca server crl

To display the current Certificate Revocation List (CRL) of the local Certificate Authority (CA) use the **show crypto ca server crl** command.

show crypto ca server crl

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example displays the current CRL the embedded CA server:

```
hostname# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
hostname#
```

Related Commands

Command	Description
cdp-url	Specifies the Certificate Revocation List (CRL) distribution point (CDP) to be include in the certificates issued by the CA.
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.

Command	Description
lifetime crl	Specifies the lifetime of the Certificate Revocation List (CRL).
show crypto ca server	Displays the status of the CA configuration.

show crypto ca server user-db

To display users included in the local Certificate Authority (CA) server user database, use the **show crypto ca server user-db** command.

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

Syntax Description

allowed	(Optional) Specifies that users who are allowed to enroll display, regardless of the status of their certificate.
enrolled	(Optional) Specifies that users with valid certificates display.
expired	(Optional) Specifies that users holding expired certificates display.
on-hold	(Optional) Specifies that users who have not enrolled yet display.

Defaults

By default, all users in the database display if no keywords are entered.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example displays currently enrolled users:

```
hostname# crypto ca server user-db enrolled
Username    DN                Certificate issued    Certificate expiration
jandoe      cn=Jan Doe,o=...  5/31/2006             5/31/2007

hostname#
```

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db allow	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
crypto ca server user-db remove	Removes a user from the CA server user database.

Command	Description
crypto ca server user-db write	Writes user information configured in the local CA database to storage..
show crypto ca server cert-db	Displays all certificates issued by the local CA.

show crypto ipsec df-bit

To display the IPSec DF-bit policy for IPSec packets for a specified interface, use the **show crypto ipsec df-bit** command in global configuration mode and privileged EXEC mode.

show crypto ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example displays the IPSec DF-bit policy for interface named inside:

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPSec DF-bit policy for IPSec packets.
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPSec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPSec packets, use the **show crypto ipsec fragmentation** command in global configuration or privileged EXEC mode.

show crypto ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, displays the IPSec fragmentation policy for an interface named inside:

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

show crypto ipsec sa

To display a list of IPSec SAs, use the **show crypto ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec sa**.

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPSec SAs sorted by peer address
identity	(Optional) Displays IPSec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPSec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPSec SAs for specified peer IP addresses.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPSec SA policy states that fragmentation occurs before IPSec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPSec processing.

The following example, entered in global configuration mode, displays IPSec SAs for a crypto map named def.

```
hostname(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
```

```
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
```

```
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

```
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example shows IPSec SAs with the keyword **identity**.

```
hostname(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPSec SAs with the keywords **identity** and **detail**.

```
hostname(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
```

```
    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
    current_peer: 10.132.0.21
    dynamic allocated peer ip: 90.135.1.5

    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68

  Crypto map tag: def, local addr: 172.20.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0

    #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
    #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec stats

To display a list of IPSec statistics, use the **show crypto ipsec stats** command in global configuration mode or privileged EXEC mode.

show crypto ipsec stats

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, displays IPSec statistics:

```
hostname(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
```

```
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Clears IPSec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPSec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPSec SAs.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

show crypto isakmp stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp sa

To display the IKE runtime SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

show crypto isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
hostname(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

show crypto isakmp stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the **show crypto protocol statistics** command in global configuration or privileged EXEC mode.

show crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which to display statistics. Protocol choices are as follows: **ikev1**—Internet Key Exchange version 1. **ipsec**—IP Security Phase-2 protocols. **ssl**—Secure Socket Layer. **other**—Reserved for new protocols. **all**—All protocols currently supported.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following examples entered in global configuration mode, display crypto accelerator statistics for specified protocols:

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
```

```
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
```

```
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.

show csc node-count

A node is any distinct source IP address or the address of a device that is on a network protected by the security appliance. The security appliance keeps track of a daily node count and communicates this to the CSC SSM for user license enforcement. To display the number of nodes for which the CSC SSM scanned traffic, use the **show csc node-count** command in privileged EXEC mode:

show csc node-count [**yesterday**]

Syntax Description

yesterday	(Optional) Shows the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight.

Defaults

By default, the node count displayed is the number of nodes scanned since midnight.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows the use of the **show csc node-count** command to display the number of nodes for which the CSC SSM has scanned traffic since midnight:

```
hostname# show csc node-count
Current node count is 1
```

This example shows the use of the **show csc node-count** command to display the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight:

```
hostname(config)# show csc node-count yesterday
Yesterday's node count is 2
```

Related Commands

csc	Sends network traffic to the CSC SSM for scanning of FTP, HTTP, POP3, and SMTP, as configured on the CSC SSM.
show running-config class-map	Show current class map configuration.

show running-config policy-map	Show current policy map configuration.
show running-config service-policy	Show current service policy configuration.

show ctiqbe

To display information about CTIQBE sessions established across the security appliance, use the **show ctiqbe** command in privileged EXEC mode.

show ctiqbe

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show ctiqbe** command displays information of CTIQBE sessions established across the security appliance. Along with **debug ctiqbe** and **show local-host**, this command is used for troubleshooting CTIQBE inspection engine issues.

Note We recommend that you have the **pager** command configured before using the **show ctiqbe** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctiqbe** command output to reach the end.

Examples

The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the security appliance. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
hostname# | show ctiqbe

Total: 1
  | LOCAL | FOREIGN | STATE | HEARTBEAT
-----------------------------------------------------------------
1 | 10.0.0.99/1117   172.29.1.77/2748 | 1 | 120
  | RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 | 1029)
```

```
|MEDIA: Device ID 27|Call ID 0
|Foreign 172.29.1.99|(1028|1029)
|Local|172.29.1.88|(26822|26823)
|-------------------------------------------
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with `RTP/RTCP: PAT xlates:` appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the security appliance does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

The following is the xlate information for these CTIBQE connections:

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
hostname#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ctiqbe	Enables CTIQBE application inspection.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show curpriv

To display the current user privileges, use the **show curpriv** command:

show curpriv

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•
Privileged EXEC	•	•	—	—	•
User EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	Modified to conform to CLI guidelines.

Usage Guidelines

The show curpriv command displays the current privilege level. Lower privilege level numbers indicate lower privilege levels.

Examples

These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in, P_PRIV indicates that the user has entered the **enable** command, and P_CONF indicates that the user has entered the **config terminal** command.

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit
```

```
hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

The following is a known behavior. When you are in enable mode then enter disable mode the initial logged in username is replaced with enable_1 as shown in the example below:

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
asa2(config)# disable
asa2> show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show running-config privilege	Display privilege levels for commands.

CHAPTER 26

show ddns update interface through show ipv6 traffic Commands

show ddns update interface

To display the DDNS methods assigned to security appliance interfaces, use the **show ddns update interface** command in privileged EXEC mode.

show ddns update interface [*interface-name*]

Syntax Description

interface-name	(Optional) The name of a network interface.

Defaults

Omitting the *interface-name* string displays the DDNS method assigned to each interface.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays the DDNS method assigned to the inside interface:

```
hostname# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
hostname#
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a security appliance interface with a DDNS update method or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

show ddns update method

To display the DDNS update methods in the running configuration, use the **show ddns update method** command in privileged EXEC mode.

show ddns update method [*method-name***]**

Syntax Description

method-name	(Optional) The name of a configured DDNS update method.

Defaults

Omitting the *method-name* string displays all configured DDNS update methods.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays the DDNS method named ddns-2:

```
hostname(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
hostname(config)#
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a security appliance interface with a Dynamic DNS (DDNS) update method or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show ddns update interface	Displays the interfaces associated with each configured DDNS method.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

show debug

To show the current debugging configuration, use the **show debug** command.

show debug [*command* [*keywords*]]

Syntax Description

command	(Optional) Specifies the debug command whose current configuration you want to view. For each *command*, the syntax following *command* is identical to the syntax supported by the associated **debug** command. For example, valid *keywords* following **show debug aaa** are the same as the valid keywords for the **debug aaa** command. Thus, **show debug aaa** supports an **accounting** keyword, which allows you to specify that you want to see the debugging configuration for that portion of AAA debugging.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.
8.0(2)	The **eigrp** keyword was added to the list of possible command values.

Usage Guidelines

The valid *command* values follow. For each *command*, the syntax following *command* is identical to the syntax supported by the associated **debug** command. Refer to the associated **debug** command for

Note The availability of each *command* value depends upon the command modes that support the applicable **debug** command.

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**

- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

Examples

The following commands enable debugging for authentication, accounting, and Flash memory. The **show debug** command is used in three ways to demonstrate how you can use it to view all debugging configuration, debugging configuration for a specific feature, and even debugging configuration for a subset of a feature.

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
```

```
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

Related Commands

Command	Description
debug	See all **debug** commands.

show debug mmp

To display current debug settings for the MMP inspection module, use the **show debug mmp** command in privileged EXEC mode.

show debug mmp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **show debug mmp** command to displaythe current debug settings for the MMP inspection module:

```
hostname# show debug mmp
debug mmp  enabled at level 1
```

Related Commands

Command	Description
debug mmp	Display inspect MMP events.
inspect mmp	Configures the MMP inspection engine.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

Syntax Description

binding	Displays binding information for a given server IP address and its associated client hardware address and lease length.
IP_address	Shows the binding information for the specified IP address.
state	Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces.
statistics	Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

Examples

The following is sample output from the **show dhcpd binding** command:

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
```

```
Interface inside, Not Configured for DHCP
```

The following is sample output from the **show dhcpd statistics** command:

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
clear dhcpd	Clears the DHCP server bindings and statistic counters.
dhcpd lease	Defines the lease length for DHCP information granted to clients.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

show dhcprelay state

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

Examples

The following is sample output from the **show dhcprelay state** command:

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

Related Commands

Command	Description
show dhcpd	Displays DHCP server statistics and state information.
show dhcprelay statistics	Displays the DHCP relay statistics.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show dhcprelay statistics

To display the DHCP relay statistics, use the **show dhcprelay statistics** command in privileged EXEC mode.

show dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples

The following shows sample output for the **show dhcprelay statistics** command:

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
hostname#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay state	Displays the state of the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show disk

To display the contents of the Flash memory for the adaptive security appliance only, use the **show disk** command in privileged EXEC mode. To display the contents of the Flash memory for a PIX security appliance only, see the **show flash** command.

show disk[**0** | **1**] [**filesys** | **all**] **controller**

Syntax Description

0 | **1**	Specifies the internal Flash memory (0, the default) or the external Flash memory (1).
controller	Specifies the Flash controller model number.
filesys	Shows information about the compact Flash card.
all	Shows the contents of Flash memory plus the file system information,

Defaults

Shows the internal Flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show disk** command:

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
```

```
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

The following is sample output from the **show disk controller** command:

```
hostname# show disk1: controller
Flash Model: TOSHIBA THNCF064MBA
```

Related Commands

Command	Description
dir	Displays the directory contents.
show flash	Displays the contents of the internal Flash memory for the PIX security appliance only.

show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode.The DNS cache includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

show dns-hosts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show dns-hosts** command:

```
hostname# show dns-hosts
Host                      Flags      Age Type   Address(es)
ns2.example.com           (temp, OK) 0    IP    10.102.255.44
ns1.example.com           (temp, OK) 0    IP    192.168.241.185
snowmass.example.com      (temp, OK) 0    IP    10.94.146.101
server.example.com        (temp, OK) 0    IP    10.94.146.80
```

Table 11 shows each field description.

Table 26-1 show dns-hosts Fields

Field	Description
Host	Shows the hostname.
Flags	Shows the entry status, as a combination of the following: • temp—This entry is temporary because it comes from a DNS server. The security appliance removes this entry after 72 hours of inactivity. • perm—This entry is permanent because it was added with the **name** command. • OK—This entry is valid. • ??—This entry is suspect and needs to be revalidated. • EX—This entry is expired.
Age	Shows the number of hours since this entry was last referenced.
Type	Shows the type of DNS record; this value is always IP.
Address(es)	The IP addresses.

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

show eigrp events

To display the EIGRP event log, use the **show eigrp events** command in privileged EXEC mode.

show eigrp [*as-number*] **events** [{*start end*} | **type**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.
end	(Optional) Limits the output to the entries with starting with the *start* index number and ending with the *end* index number.
start	(Optional) A number specifying the log entry index number. Specifying a start number causes the output to start with the specified event and end with the event specified by the *end* argument. Valid values are from 1 to 4294967295.
type	(Optional) Displays the events that are being logged.

Defaults

If a *start* and *end* is not specified, all log entries are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **show eigrp events** output displays up to 500 events. Once the maximum number of events has been reached, new events are added to the bottom of the output and old events are removed from the top of the output.

You can use the **clear eigrp events** command to clear the EIGRP event log.

The **show eigrp events type** command displays the logging status of EIGRP events. By default, neighbor changes, neighbor warning, and DUAL FSM messages are logged. You can disable neighbor change event logging using the **no eigrp log-neighbor-changes** command. You can disable neighbor warning event logging using the **no eigrp log-neighbor-warnings** command. You cannot disable the logging of DUAL FSM events.

Examples

The following is sample output from the **show eigrp events** command:

```
hostname# show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command with a start and stop number defined:

```
hostname# show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command when there are no entries in the EIGRP event log:

```
hostname# show eigrp events

Event information for AS 100:  Event log is empty.
```

The following is sample output from the **show eigrp events type** command:

```
hostname# show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

Related Commands

Command	Description
clear eigrp events	Clears the EIGRP event logging buffer.
eigrp log-neighbor-changes	Enables the logging of neighbor change events.
eigrp log-neighbor-warnings	Enables the logging of neighbor warning events.

show eigrp interfaces

To display the interfaces participating in EIGRP routing, use the **show eigrp interfaces** command in privileged EXEC mode.

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are displaying active interfaces. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name limits the display to the specified interface.

Defaults

If you do not specify an interface name, information for all EIGRP interfaces is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **show eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show eigrp interfaces** command:

```
hostname# show eigrp interfaces

EIGRP-IPv4 interfaces for process 100

                   Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers  Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
```

```
mgmt          0          0/0           0       11/434           0           0
outside       1          0/0         337        0/10            0           0
inside        1          0/0          10        1/63          103           0
```

Table 26-2 describes the significant fields shown in the display.

Table 26-2 show eigrp interfaces Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Peers	Number of directly-connected peers.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the security appliance will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
network	Defines the networks and interfaces that participate in the EIGRP routing process.

show eigrp neighbors

To display the EIGRP neighbor table, use the **show eigrp neighbors** command in privileged EXEC mode.

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail neighbor information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name displays all neighbor table entries that were learned through that interface.
static	(Optional) Displays EIGRP neighbors that are statically defined using the **neighbor** command.

Defaults

If you do not specify an interface name, the neighbors learned through all interfaces are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **clear eigrp neighbors** command to clear the dynamically-learned neighbors from the EIGRP neighbor table.

Static neighbors are not included in the output unless you use the **static** keyword.

Examples

The following is sample output from the **show eigrp neighbors** command:

```
hostname# show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100
Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
```

```
172.16.80.28            Ethernet0     14        0:02:01  0       10    12    24
172.16.80.31            Ethernet0     12        0:02:02  0       4     5     20
```

Table 26-2 describes the significant fields shown in the display.

Table 26-3 show eigrp neighbors Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the security appliance receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the security appliance waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the security appliance considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the security appliance first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the security appliance is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the security appliance to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the security appliance waits before resending a packet from the retransmission queue to a neighbor.

The following is sample output from the **show eigrp neighbors static** command:

```
hostname# show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
Static Address                Interface
192.168.1.5                   management
```

Table 26-4 describes the significant fields shown in the display.

Table 26-4 show ip eigrp neighbors static Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.

Table 26-4 show ip eigrp neighbors static Field Descriptions

Field	Description
Static Address	IP address of the EIGRP neighbor.
Interface	Interface on which the security appliance receives hello packets from the neighbor.

The following is sample output from the **show eigrp neighbors detail** command:

```
hostname# show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 26-5 describes the significant fields shown in the display.

Table 26-5 show ip eigrp neighbors details Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the security appliance receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the security appliance waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the security appliance considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the security appliance first heard from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the security appliance to receive an acknowledgment of that packet.

Table 26-5 show ip eigrp neighbors details Field Descriptions

Field	Description
RTO	Retransmission timeout (in milliseconds). This is the amount of time the security appliance waits before resending a packet from the retransmission queue to a neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the security appliance is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.
Retries	The number of times an attempt was made to retransmit a packet.
Restart time	Elapsed time (in hours:minutes: seconds) since the specified neighbor has restarted.

Related Commands

Command	Description
clear eigrp neighbors	Clear the EIGRP neighbor table.
debug eigrp neighbors	Display EIGRP neighbor debug messages.
debug ip eigrp	Display EIGRP packet debug messages.

show eigrp topology

To display the EIGRP topology table, use the **show eigrp topology** command in privileged EXEC mode.

show eigrp [*as-number*] **topology [***ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

Syntax Description

active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all routes in the EIGRP topology table, even those that are not feasible successors.
as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.
ip-addr	(Optional) The IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided.
mask	(Optional) The network mask to apply to the *ip-addr* argument.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

Defaults

Only routes that are feasible successors are displayed. Use the **all-links** keyword to display all routes, including those that are not feasible successors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **clear eigrp topology** command to remove the dynamic entries from the topology table.

Examples

The following is sample output from the **show eigrp topology** command:

```
hostname# show eigrp topology

EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
```

```
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.16.90.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.16.81.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

Table 26-6 describes the significant fields shown in the displays.

Table 26-6 show eigrp topology Field Information

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P - Passive	The route is known to be good and no EIGRP computations are being performed for this destination.
A - Active	EIGRP computations are being performed for this destination.
U - Update	Indicates that an update packet was sent to this destination.
Q - Query	Indicates that a query packet was sent to this destination.
R - Reply	Indicates that a reply packet was sent to this destination.
r - Reply status	Flag that is set after the software has sent a query and is waiting for a reply.
address mask	Destination IP address and mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
via	IP address of the peer that told the software about this destination. The first *n* of these entries, where *n* is the number of successors, is the current successors. The remaining entries on the list are feasible successors.
(*cost*/*adv_cost*)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.
interface	The interface from which the information was learned.

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an internal route.

```
hostname# show eigrp topology 10.2.1.0 255.255.255.0

EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0
```

```
    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an external route.

```
hostname# show eigrp topology 10.4.80.0 255.255.255.0


EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
            External data:
                Originating router is 10.89.245.1
                AS number of route is 0
                External protocol is Connected, external metric is 0
                Administrator tag is 0 (0x00000000)
```

Related Commands

Command	Description
clear eigrp topology	Clears the dynamically discovered entries from the EIGRP topology table.

show eigrp traffic

To display the number of EIGRP packets sent and received, use the **show eigrp traffic** command in privileged EXEC mode.

show eigrp [*as-number*] **traffic**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the security appliance only supports one EIGRP routing process, you do not need to specify the autonomous system number.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **clear eigrp traffic** command to clear the EIGRP traffic statistics.

Examples

The following is sample output from the **show eigrp traffic** command:

```
hostname# show eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

Table 26-4 describes the significant fields shown in the display.

Table 26-7 show eigrp traffic Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.
Input queue high water mark/drops	Number of received packets that are approaching the maximum receive threshold and number of dropped packets.
SIA-Queries sent/received	Stuck in active queries sent and received.
SIA-Replies sent/received	Stuck in active replies sent and received.

Related Commands

Command	Description
debug eigrp packets	Displays debug information for EIGRP packets sent and received.
debug eigrp transmit	Displays debug information for EIGRP messages sent.

show failover

To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

Syntax Description

group	Displays the running state of the specified failover group.
history	Displays failover history. The failover history displays past failover state changes and the reason for the state change. History information is cleared with the device is rebooted.
interface	Displays failover command and stateful link information.
num	Failover group number.
state	Displays the failover state of both failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover. The fail reason remains in the output even when the reason for failure is cleared.
statistics	Displays transmit and receive packet count of failover command interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified. The output includes additional information.

Usage Guidelines

The **show failover** command displays the dynamic failover information, interface status, and Stateful Failover statistics. The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled. The “xerr” and “rerr” values do not indicate errors in failover, but rather the number of packet transmit or receive errors.

Note Stateful Failover, and therefore Stateful Failover statistics output, is not available on the ASA 5505 adaptive security appliance.

In the **show failover** command output, the stateful failover fields have the following values:

- Stateful Obj has these values:
  - xmit—Indicates the number of packets transmitted.
  - xerr—Indicates the number of transmit errors.
  - rcv—Indicates the number of packets received.
  - rerr—Indicates the number of receive errors.
- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - sys cmd—Refers to the logical update system commands, such as **login** or **stay alive**.
  - up time—Indicates the value for the security appliance up time, which the active security appliance passes on to the standby security appliance.
  - RPC services—Remote Procedure Call connection information.
  - TCP conn—Dynamic TCP connection information.
  - UDP conn—Dynamic UDP connection information.
  - ARP tbl—Dynamic ARP table information.
  - Xlate_Timeout—Indicates connection translation timeout information.
  - VPN IKE upd—IKE connection information.
  - VPN IPSEC upd—IPSec connection information.
  - VPN CTCP upd—cTCP tunnel connection information.
  - VPN SDI upd—SDI AAA connection information.
  - VPN DHCP upd—Tunneled DHCP connection information.
  - SIP Sesson—SIP signalling session information.

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a “waiting” state. You must set a failover IP address for failover to work.

Table 26-8 describes the interface states for failover.

Table 26-8 Failover Interface States

State	Description
Normal	The interface is up and receiving hello packets from the corresponding interface on the peer unit.
Normal (Waiting)	The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Normal (Not-Monitored)	The interface is up but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
No Link	The physical link is down.
No Link (Waiting)	The physical link is down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After restoring the link, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.

Table 26-8 Failover Interface States (continued)

State	Description
No Link (Not-Monitored)	The physical link is down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Link Down	The physical link is up, but the interface is administratively down.
Link Down (Waiting)	The physical link is up, but the interface is administratively down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After bringing the interface up (using the **no shutdown** command in interface configuration mode), verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Link Down (Not-Monitored)	The physical link is up, but the interface is administratively down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Testing	The interface is in testing mode due to missed hello packets from the corresponding interface on the peer unit.
Failed	Interface testing has failed and the interface is marked as failed. If the interface failure causes the failover criteria to be met, then the interface failure causes a failover to the secondary unit or failover group.

In multiple configuration mode, only the **show failover** command is available in a security context; you cannot enter the optional keywords.

Examples

The following is sample output from the **show failover** command for Active/Standby Failover. The security appliances are ASA 5500 series adaptive security appliances, each equipped with a CSC SSM as shown in the details for slot 1 of each security appliance.

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3): Normal
                  Interface outside (10.132.9.3): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4): Normal
                  Interface outside (10.132.9.4): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status (Up/Up)
```

```
                Logging port IP: 10.0.0.4/24
                CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
       SIP Session    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

The following is sample output from the **show failover** command for Active/Active Failover:

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)
```

```
                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
       SIP Session    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

The following is sample output from the **show failover** command on the ASA 5505 series adaptive security appliance:

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

The following is sample output from the **show failover state** command:

```
hostname# show failover state

====My State===
Primary | Active |
====Other State===
Secondary | Standby |
====Configuration State===
        Sync Done
====Communication State===
        Mac set
=========Failed Reason==============
My Fail Reason:
Other Fail Reason:
        Service Card Failure
```

Table 26-9 describes the output of the **show failover state** command.

Table 26-9 show failover state Output Description

Field	Description
My State	Displays the Primary/Secondary and Active/Standby status for the unit.
Other State	Displays the Primary/Secondary and Active/Standby status for peer unit.
Configuration State	Displays the state of configuration synchronization. The following are possible configuration states for the standby unit: • **Config Syncing - STANDBY**—Set while the synchronized configuration is being executed. • **Sync Done - STANDBY**—Set when the standby unit has completed a configuration synchronization from the active unit. The following are possible configuration states for the active unit: • **Config Syncing**—Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Sync Done**—Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**—Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.

Table 26-9 show failover state Output Description (continued)

Field	Description
Communication State	Displays the status of the MAC address synchronization. • **Mac set**—The MACs have been synchronized from the peer unit to this unit. • **Updated Mac**—Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Failed Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information only changes when a failover occurs. The following are possible fail reasons: • **Ifc Failure**—The number of interfaces that failed met the failover criteria and caused failover. • **Comm Failure**—The failover link failed or peer is down. • **Service card Failure**—The SSM card failed (ASA only).

The following is sample output from the **show failover history** command:

```
hostname# show failover history

==========================================================================
From State                To State                  Reason
==========================================================================
At   16:28:50 UTC Sep 9 2006
Not Detected              Negotiation               No Error

At   16:29:18 UTC Sep 9 2006
Negotiation               Cold Standby              Detected an Active mate

At   16:29:19 UTC Sep 9 2006
Cold Standby              Sync Config               Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync Config               Sync File System          Detected an Active mate

At   16:29:31 UTC Sep 9 2006
Sync File System          Bulk Sync                 Detected an Active mate

At   16:29:36 UTC Sep 9 2006
Bulk Sync                 Standby Ready             Detected an Active mate

At   16:30:52 UTC Sep 9 2006
Standby Ready             Just Active               Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Just Active               Active Drain              Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Drain              Active Applying Config    Set by the CI config cmd

At   16:30:52 UTC Sep 9 2006
Active Applying Config    Active Config Applied     Set by the CI config cmd
```

```
At   16:30:52 UTC Sep 9 2006
Active Config Applied      Active                    Set by the CI config cmd

At   16:30:55 UTC Sep 9 2006
Active                     Disabled                  Set by the CI config cmd

================================================================================
```

Each entry provides the time and date the state change occurred, the beginning state, the resulting state, and the reason for the state change. The newest entries are located at the bottom of the display. Older entries appear at the top. A maximum of 60 entries can be displayed. Once the maximum number of entries has been reached, the oldest entries are removed from the top of the output as new entries are added to the bottom.

Table 26-10 shows the failover states. There are two types of states—stable and transient. Stable states are states that the unit can remain in until some occurrence, such as a failure, causes a state change. A transient state is a state that the unit passes through while reaching a stable state.

Table 26-10 Failover States

State	Description
Initialization	The unit checks platform capabilities and configuration and prepares the failover communication channels. This is a transient state.
Disabled	Failover is disabled. This is a stable state.
Negotiation	The unit establishes the connection with peer and negotiates with peer to determine software version compatibility and Active/Standby role. Depending upon the role that is negotiated, the unit will go through the Standby Unit States or the Active Unit States or enter the failed state. This is a transient state.
Failed	The unit is in the failed state. This is a stable state.
Standby Unit States	
Cold Standby	The unit waits for the peer to reach the Active state. When the peer unit reaches the Active state, this unit progresses to the Standby Config state. This is a transient state.
Sync Config	The unit requests the running configuration from the peer unit. If an error occurs during the configuration synchronization, the unit returns to the Initialization state. This is a transient state.
Sync File System	The unit synchronizes the file system with the peer unit. This is a transient state.
Bulk Sync	The unit receives state information from the peer. This state only occurs when Stateful Failover is enabled. This is a transient state.
Standby Ready	The unit is ready to take over if the active unit fails. This is a stable state.
Active Unit States	
Just Active	The first state the unit enters when becoming the active unit. During this state a message is sent to the peer alerting the peer that the unit is becoming active and the IP and MAC addresses are set for the interfaces. This is a transient state.
Active Drain	Queues messages from the peer are discarded. This is a transient state.
Active Applying Config	The unit is applying the system configuration. This is a transient state.

Table 26-10 Failover States

State	Description
Active Config Applied	The unit has finished applying the system configuration. This is a transient state.
Active	The unit is active and processing traffic. This is a stable state.

Each state change is followed by a reason for the state change. The reason typically remains the same as the unit progresses through the transient states to the stable state. The following are the possible state change reasons:

- No Error
- Set by the CI config cmd
- Failover state check
- Failover interface become OK
- HELLO not heard from mate
- Other unit has different software version
- Other unit operating mode is different
- Other unit license is different
- Other unit chassis configuration is different
- Other unit card configuration is different
- Other unit want me Active
- Other unit want me Standby
- Other unit reports that I am failed
- Other unit reports that it is failed
- Configuration mismatch
- Detected an Active mate
- No Active unit found
- Configuration synchronization done
- Recovered from communication failure
- Other unit has different set of vlans configured
- Unable to verify vlan configuration
- Incomplete configuration synchronization
- Configuration synchronization failed
- Interface check
- My communication failed
- ACK not received for failover message
- Other unit got stuck in learn state after sync
- No power detected from peer
- No failover cable

- HA state progression failed
- Detect service card failure
- Service card in other unit has failed
- My service card is as good as peer
- LAN Interface become un-configured
- Peer unit just reloaded
- Switch from Serial Cable to LAN-Based fover
- Unable to verify state of config sync
- Auto-update request
- Unknown reason

Related Commands

Command	Description
show running-config failover	Displays the **failover** commands in the current configuration.

show failover exec

To display the **failover exec** command mode for the specified unit, use the **show failover exec** command in privileged EXEC mode.

show failover exec {**active** | **standby** | **mate**}

Syntax Description

active	Displays the **failover exec** command mode for the active unit.
mate	Displays the **failover exec** command mode for the peer unit.
standby	Displays the **failover exec** command mode for the standby unit.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode. You can change the command mode of that session by sending the appropriate command (such as the **interface** command) using the **failover exec** command. Changing **failover exec** command modes for the specified device does not change the command mode for the session you are using to access the device. Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command.

The **show failover exec** command displays the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Examples

The following is sample output from the **show failover exec** command. This example demonstrates that the command mode for the unit where the **failover exec** commands are being entered does not have to be the same as the **failover exec** command mode where the commands are being executed.

In this example, an administrator logged into the standby unit adds a name to an interface on the active unit. The second time the **show failover exec mate** command is entered in this example shows the peer device in interface configuration mode. Commands sent to the device with the **failover exec** command are executed in that mode.

```
hostname(config)# show failover exec mate
```

```
Active unit Failover EXEC is at config mode

! The following command changes the standby unit failover exec mode
! to interface configuration mode.
hostname(config)# failover exec mate interface GigabitEthernet0/1
hostname(config)# show failover exec mate

Active unit Failover EXEC is at interface sub-command mode

! Because the following command is sent to the active unit, it is replicated
! back to the standby unit.
hostname(config)# failover exec mate nameif test
```

Related Commands

Command	Description
failover exec	Executes the supplied command on the designated unit in a failover pair.

show file

To display information about the file system, use the **show file** command in privileged EXEC mode.

show file descriptors | system | information *filename*

Syntax Description

descriptors	Displays all open file descriptors.
information	Displays information about a specific file.
filename	Specifies the filename.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to display the file system information:

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

Related Commands

Command	Description
dir	Displays the directory contents.
pwd	Displays the current working directory.

show firewall

To show the current firewall mode (routed or transparent), use the **show firewall** command in privileged EXEC mode.

show firewall

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show firewall** command:

```
hostname# show firewall
Firewall mode: Router
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode.
show mode	Shows the current context mode, either single or multiple.

show flash

To display the contents of the internal Flash memory, use the **show flash:** command in privileged EXEC mode.

show flash:

Note In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to display the contents of the internal Flash memory:

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
```

```
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

Related Commands

Command	Description
dir	Displays the directory contents.
show disk0	Displays the contents of the internal Flash memory.
show disk1	Displays the contents of the external Flash memory card.

show fragment

To display the operational data of the IP fragment reassembly module, enter the **show fragment** command in privileged EXEC mode.

show fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an *interface* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data.

Examples

This example shows how to display the operational data of the IP fragment reassembly module:

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.

Command	Description
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show gc

To display the garbage collection process statistics, use the **show gc** command in privileged EXEC mode.

show gc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show gc** command:

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :             0
Total udp conn delete response             :             0
Total number of zombie cleaned             :             0
Total number of embryonic conn cleaned     :             0
Total error response                       :             0
Total queries generated                    :             0
Total queries with conn present response   :             0
Total number of sweeps                     :           946
Total number of invalid vcid               :             0
Total number of zombie vcid                :             0
```

Related Commands

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

To display information for H.225 sessions established across the security appliance, use the **show h225** command in privileged EXEC mode.

show h225

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the security appliance. Along with the **debug h323 h225 event**, **debug h323 h245 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Before using the **show h225**, **show h245**, or **show h323-ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end. If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

Examples

The following is sample output from the **show h225** command:

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
  Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local: 10.130.56.3/1040 Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
  Local: 10.130.56.4/1050 Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the security appliance between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV (Call Reference Value) for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent Calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set "maintainConnection" to TRUE, so the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h245

To display information for H.245 sessions established across the security appliance by endpoints using slow start, use the **show h245** command in privileged EXEC mode.

show h245

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the security appliance by endpoints using slow start. (Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Examples

The following is sample output from the **show h245** command:

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the security appliance. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. (The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives

the length of the message, including the 4-byte header.) The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have a LCN (logical channel number) of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and a RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and a RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and a RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h323-ras

To display information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint, use the **show h323-ras** command in privileged EXEC mode.

show h323-ras

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show h323-ras** command displays information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

The **show h323-ras** command displays connection information for troubleshooting H.323 inspection engine issues, and is described in the **inspect protocol h323 {h225 | ras}** command page.

Examples

The following is sample output from the **show h323-ras** command:

```
hostname# show h323-ras
Total: 1
  GK  Caller
  172.30.254.214 10.130.56.14
hostname#
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show history

To display the previously entered commands, use the **show history** command in user EXEC mode.

show history

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show history** command lets you display previously entered commands. You can examine commands individually with the up and down arrows, enter **^p** to display previously entered lines, or enter **^n** to display the next line.

Examples

The following example shows how to display previously entered commands when you are in user EXEC mode:

```
hostname> show history
    show history
    help
    show history
```

The following example shows how to display previously entered commands in privileged EXEC mode:

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

This example shows how to display previously entered commands in global configuration mode:

```
hostname(config)# show history
    show history
    help
```

```
show history
enable
show history
config t
show history
```

Related Commands

Command	Description
help	Displays help information for the command specified.

show icmp

To display the ICMP configuration, use the **show icmp** command in privileged EXEC mode.

show icmp

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was previously existing.

Usage Guidelines

The **show icmp** command displays the ICMP configuration.

Examples

The following example shows the ICMP configuration:

```
hostname# show icmp
```

Related Commands

clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
inspect icmp	Enables or disables the ICMP inspection engine.
timeout icmp	Configures the idle timeout for ICMP.

show idb

To display information about the status of interface descriptor blocks, use the **show idb** command in privileged EXEC mode.

show idb

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

IDBs are the internal data structure representing interface resources. See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show idb** command:

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
              Active 6          21
            Inactive 1          2
          Total IDBs 7          23
 Size each (bytes) 116          212
        Total bytes 812         4876

HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0

SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
```

```
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

Table 26-1 shows each field description.

Table 26-11 show idb stats Fields

Field	Description
HWIDBs	Shows the statistics for all HWIDBs. HWIDBs are created for each hardware port in the system.
SWIDBs	Shows the statistics for all SWIDBs. SWIDBs are created for each main and subinterface in the system, and for each interface that is allocated to a context. Some other internal software modules also create IDBs.
HWIDB#	Specifies a hardware interface entry. The IDB sequence number, address, and interface name is displayed in each line.
SWIDB#	Specifies a software interface entry. The IDB sequence number, address, corresponding vPif id, and interface name are displayed in each line.
PEER IDB#	Specifies an interface allocated to a context. The IDB sequence number, address, corresponding vPif id, context id and interface name are displayed in each line.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show igmp groups

To display the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP, use the **show igmp groups** command in privileged EXEC mode.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	(Optional) Provides a detailed description of the sources.
group	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
if_name	(Optional) Displays group information for the specified interface.
reserved	(Optional) Displays information about reserved groups.
summary	(Optional) Displays group joins summary information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

The following is sample output from the **show igmp groups** command:

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command in privileged EXEC mode.

show igmp interface [*if_name*]

Syntax Description

if_name	(Optional) Displays IGMP group information for the selected interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was modified. The **detail** keyword was removed.

Usage Guidelines

If you omit the optional *if_name* argument, the **show igmp interface** command displays information about all interfaces.

Examples

The following is sample output from the **show igmp interface** command:

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.

show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command in privileged EXEC mode.

show igmp traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show igmp traffic** command:

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP statistic counters.
clear igmp traffic	Clear the IGMP traffic counters.

show import webvpn

To list the WebVPN custom data and plug-ins that currently are present in flash memory on the security appliance, enter the **show import webvpn (***option***)** command in privileged EXEC mode.

show import webvpn | customization | plug-in | translation-table | url-list | webcontent

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **show import webvpn** command to identify the custom data and the Java-based client applications available to WebVPN users. The displayed list itemizes all of the requested data types that are in flash memory on the security appliance.

Each of the show import webvpn command displays the following currently loaded WebVPN data:

- Customization - customization object (file names base64 decoded)
- Plug-in - Third-party Java-based client applications (SSH, VNC, and RDP)
- Translation Table - Localization/internationalization dictionary tables
- URL-list - URL list objects (file names base64 decoded)
- Web content - disk0:/csco_config/htms recursively (all files full names)

Example

The following illustrates the WebVPN data displayed by various **show import webvpn** command:

```
hostname# show import webvpn plug-in
ssh
rdp
vnc
hostname#

hostname# show import webvpn customization
Template
```

```
DfltCustomization
hostname#

hostname# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
hostname#

hostname# show import webvpn url-list
Template
No bookmarks are currently defined
hostname#

hostname# show import webvpn webcontent
No custom webcontent is loaded
hostname#
```

Related Commands

Command	Description
revert webvpn all	Removes all WebVPN data and plug-in current on the security appliance.

show interface

To view interface statistics, use the **show interface** command in privileged EXEC mode.

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [**stats** | **detail**]

Syntax Description

detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled by the **asr-group** command. If you show all interfaces, then information about the internal interfaces for SSMs displays, if installed on the ASA 5500 series adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet 0/1**. See the **interface** command for accepted values.
redundant*number*	(Optional) Identifies the redundant interface ID, such as **redundant1**.
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Defaults

If you do not identify any options, this command shows basic statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword.
7.0(4)	This command added support for the 4GE SSM interfaces.

Release	Modification
7.2(1)	This command added support for switch interfaces.
8.0(2)	This command added support for redundant interfaces. Also, the delay is added for subinterfaces. Two new counters were added: input reset drops and output reset drops.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the security appliance shows only statistics for the current context. When you enter this command in the system execution space for a physical interface, the security appliance shows the combined statistics for all contexts.

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context. If you set the **visible** keyword in the **allocate-interface** command, the security appliance shows the interface ID in the output of the **show interface** command.

Note The number of bytes transmitted or received in the Hardware count and the Traffic Statistics count are different.

In the hardware count, the amount is retrieved directly form hardware, and reflects the Layer 2 packet size. While in traffic statistics, it reflects the Layer 3 packet size.

The count difference is varied based upon the design of the interface card hardware.

For example, for a Fast Ethernet card, the Layer 2 count is 14 bytes greater than the traffic count, because it includes the Ethernet header. On the Gigabit Ethernet card, the Layer 2 count is 18 bytes greater than the traffic count, because it includes both the Ethernet header and the CRC.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show interface** command:

```
hostname# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
```

```
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
```

```
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

Table 26-1 shows each field description.

Table 26-12 show interface Fields

Field	Description
Interface *ID*	The interface ID. Within a context, the security appliance shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword.
"*interface_name*"	The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.
Line protocol is *state*	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinterfaces, the VLAN ID.
Hardware	The interface type, maximum bandwidth, delay, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses. The following list describes the common hardware types: • i82542 - Intel PCI Fiber Gigabit card used on PIX platforms • i82543 - Intel PCI-X Fiber Gigabit card used on PIX platforms • i82546GB - Intel PCI-X Copper Gigabit used on ASA platforms • i82547GI - Intel CSA Copper Gigabit used as backplane on ASA platforms • i82557 - Intel PCI Copper Fast Ethernet used on ASA platforms • i82559 - Intel PCI Copper Fast Ethernet used on PIX platforms • VCS7380 - Vitesse Four Port Gigabit Switch used in SSM-4GE
Media-type	(For 4GE SSM interfaces only) Shows if the interface is set as RJ-45 or SFP.

message area	A message might be displayed in some circumstances. See the following examples:
	• In the system execution space, you might see the following message:
	`Available for allocation to a context`
	• If you do not configure a name, you see the following message:
	`Available but not configured via nameif`
	• If an interface is a member of a redundant interface, you see the following message:
	`Active member of Redundant5`

MAC address	The interface MAC address.

Table 26-12 show interface Fields (continued)

Field	Description
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows "MTU not set."
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows "IP address unassigned" because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of received packets discarded because there was no buffer space in the main system. Compare this with the ignored count. Broadcast storms on Ethernet networks are often responsible for no input buffer events.
Received:	
Broadcasts	The number of broadcasts received.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the security appliance notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the security appliance was incapable of handing received data to a hardware buffer because the input rate exceeded the security appliance capability to handle the data.
Ignored	This field is not used. The value is always 0.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured (**nameif** command) or a frame with an invalid VLAN id is received.
Packets output	The number of packets sent on this interface.
Bytes	The number of bytes sent on this interface.

Table 26-12 show interface Fields (continued)

Field	Description
Underruns	The number of times that the transmitter ran faster than the security appliance could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the security appliance resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. (“babble” means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
input reset drops	Counts the number of packets dropped in the RX ring when a reset occurs.
output reset drops	Counts the number of packets dropped in the TX ring when a reset occurs.
Rate limit drops	(For 4GE SSM interfaces only) The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration..
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.
Input queue (curr/max packets):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.

Table 26-12 show interface Fields (continued)

Field	Description
Output queue (curr/max packets):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
Traffic Statistics:	The number of packets received, transmitted, or dropped.
Packets input	The number of packets received and the number of bytes.
Packets output	The number of packets transmitted and the number of bytes.
Packets dropped	The number of packets dropped. Typically this counter increments for packets dropped on the accelerated security path (ASP), for example, if a packet is dropped due to an access list deny. See the **show asp drop** command for reasons for potential drops on an interface.
1 minute input rate	The number of packets received in packets/sec and bytes/sec over the last minute.
1 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last minute.
1 minute drop rate	The number of packets dropped in packets/sec over the last minute.
5 minute input rate	The number of packets received in packets/sec and bytes/sec over the last 5 minutes.
5 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last 5 minutes.
5 minute drop rate	The number of packets dropped in packets/sec over the last 5 minutes.
Redundancy Information:	For redundant interfaces, shows the member physical interfaces. The active interface has "(Active)" after the interface ID. If you have not yet assigned members, you see the following output: `Members unassigned`
Last switchover	For redundant interfaces, shows the last time the active interface failed over to the standby interface.

The following is sample output from the **show interface** command on the ASA 5505 adaptive security appliance, which includes switch ports:

```
hostname# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

Table 26-14 shows each field description for the **show interface** command for switch interfaces, such as those for the ASA 5505 adaptive security appliance. See Table 26-1 for fields that are also shown for the **show interface** command.

Table 26-13 show interface for Switch Interfaces Fields

Field	Description
switch ingress policy drops	This drop is usually seen when a port is not configured correctly. This drop is incremented when a packet cannot be successfully forwarded within switch ports as a result of the default or user configured switch port settings. The following configurations are the likely reasons for this drop: • The **nameif** command was not configured on the VLAN interface. **Note** For interfaces in the same VLAN, even if the **nameif** command was not configured, switching within the VLAN is successful, and this counter does not increment. • The VLAN is shut down. • An access port received an 802.1Q-tagged packet. • A trunk port received a tag that is not allowed or an untagged packet. • The security appliance is connected to another Cisco device that has Ethernet keepalives. For example, Cisco IOS software uses Ethernet loopback packets to ensure interface health. This packet is not intended to be received by any other device; the health is ensured just by being able to send the packet. These types of packets are dropped at the switch port, and the counter increments. • The VLAN only has one physical interface, but the DEST of the packet does not match the MAC address of the VLAN, and it is not the broadcast address.
switch egress policy drops	Not currently in use.

The following is sample output from the **show interface detail** command. The following example shows detailed interface statistics for all interfaces, including the internal interfaces (if present for your platform) and asymmetrical routing statistics, if enabled by the **asr-group** command:

```
hostname# show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runs, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
```

```
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

Table 26-14 shows each field description for the **show interface detail** command. See Table 26-1 for fields that are also shown for the **show interface** command.

Table 26-14 show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the security appliance was unable to demultiplex packets from SSM interfaces. SSM interfaces communicate with the native interfaces across the backplane, and packets from all SSM interfaces are multiplexed on the backplane.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down with the **shutdown** command.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the security appliance brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
delay	Changes the delay metric for an interface.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show interface ip brief

To view interface IP addresses and status, use the **show interface ip brief** command in privileged EXEC mode.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Defaults

If you do not specify an interface, the security appliance shows all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent[1]	Single	Context	System
Privileged EXEC	•	•	•	•	—

1. Available for the Management 0/0 interface or subinterface only.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command added support for VLAN interfaces, and for the Management 0/0 interface or subinterface in transparent mode.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip brief** command:

```
hostname# show interface ip brief
```

```
Interface                  IP-Address      OK? Method  Status                Protocol
Control0/0                 127.0.1.1       YES CONFIG  up                    up
GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
GigabitEthernet0/1         unassigned      YES unset   administratively down down
GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
Management0/0              209.165.201.3   YES CONFIG  up
```

Table 26-14 shows each field description.

Table 26-15 show interface ip brief Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. If you show all interfaces, then information about the internal interface for the AIP SSM displays, if installed on the ASA adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.
OK?	This column is not currently used, and always shows “Yes.”
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show inventory

To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command in user EXEC or privileged EXEC mode. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

show inventory [**slot**]

Syntax Description

slot	(Optional) Specifies the SSM slot number (the system is slot 0)

Defaults

If you do not specify a slot to show inventory for:

- Show inventory information of all SSMs (including for power supply)

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	Minor semantic changes.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in a router that are assigned a PID.

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC   , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999
```

Table 26-16describes the fields shown in the display.

Table 26-16 show inventory Field Descriptions

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.

show ip address

To view interface IP addresses or, for transparent mode, the management IP address, use the **show ip address** command in privileged EXEC mode.

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Defaults

If you do not specify an interface, the security appliance shows all interface IP addresses.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command added support for VLAN interfaces.

Usage Guidelines

This command shows the primary IP addresses (called “System” in the display) for when you configure high availability as well as the current IP addresses. If the unit is active, then the system and current IP addresses match. If the unit is standby, then the current IP addresses show the standby addresses.

Examples

The following is sample output from the **show ip address** command:

```
hostname# show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
```

```
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

Table 26-14 shows each field description.

Table 26-17 show ip address Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command.
Name	The interface name set with the **nameif** command.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.
show interface ip brief	Shows the interface IP address and status.

show ip address dhcp

To view detailed information about the DHCP lease or server for an interface, use the **show ip address dhcp** command in privileged EXEC mode.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
lease	Shows information about the DHCP lease.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
server	Shows information about the DHCP server.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent[1]	Single	Context	System
Privileged EXEC	•	—	•	•	—

1. Available for the Management 0/0 interface or subinterface only.

Command History

Release	Modification
7.0(1)	This command was changed to include the **lease** and **server** keywords to accommodate the new server functionality.
7.2(1)	This command added support for VLAN interfaces, and for the Management 0/0 interface or subinterface in transparent mode.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip address dhcp lease** command:

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
```

```
DHCP Lease server:209.165.200.225, state:3 Bound
DHCP Transaction id:0x4123
Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
Temp default-gateway addr:209.165.201.1
Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
Next timer fires after:111797 secs
Retry count:0, Client-ID:cisco-0000.0000.0000-outside
Proxy: TRUE  Proxy Network: 10.1.1.1
Hostname: device1
```

Table 26-14 shows each field description.

Table 26-18 show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the security appliance begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The security appliance is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The security appliance is waiting to hear back from the server to which it sent its request. • Purging—The security appliance is removing the lease because the client has released the IP address or there was some other error. • Bound—The security appliance has a valid lease and is operating normally. • Renewing—The security appliance is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The security appliance failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The security appliance started the process to remove the lease. • Releasing—The security appliance sends release messages to the server indicating that the IP address is no longer needed.
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.

Table 26-18 show ip address dhcp lease Fields (continued)

Field	Description
Rebind	The length of time until the security appliance attempts to rebind to a DHCP server. Rebinding occurs if the security appliance cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The security appliance then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.
Retry count	If the security appliance is attempting to establish a lease, this field shows the number of times the security appliance tried sending a DHCP message. For example, if the security appliance is in the Selecting state, this value shows the number of times the security appliance sent discover messages. If the security appliance is in the Requesting state, this value shows the number of times the security appliance sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

The following is sample output from the **show ip address dhcp server** command:

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

Table 26-19 shows each field description.

Table 26-19 show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.

Table 26-19 show ip address dhcp server Fields (continued)

Field	Description
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgements received from the server.
Naks	The number of negative acknowledgements received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip address pppoe

To view detailed information about the PPPoE connection, use the **show ip address pppoe** command in privileged EXEC mode.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} **pppoe**

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent[1]	Single	Context	System
Privileged EXEC	•	•	•	•	—

1. Available for the Management 0/0 interface or subinterface only.

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip address pppoe** command:

```
hostname# show ip address outside pppoe
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address ppoe	Sets the interface to obtain an IP address from a PPPoE server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command in privileged EXEC mode.

show ip audit count [**global | interface** *interface_name*]

Syntax Description

global	(Default) Shows the number of matches for all interfaces.
interface *interface_name*	(Optional) Shows the number of matches for the specified interface.

Defaults

If you do not specify a keyword, this command shows the matches for all interfaces (**global**).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To create an audit policy, use the **ip audit name** command, and to apply the policy, use the **ip audit interface** command.

Examples

The following is sample output from the **show ip audit count** command:

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

Related Commands

Command	Description
clear ip audit count	Clears the count of signature matches for an audit policy.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

show ip verify statistics

To show the number of packets dropped because of the Unicast RPF feature, use the **show ip verify statistics** command in privileged EXEC mode. Use the **ip verify reverse-path** command to enable Unicast RPF.

show ip verify statistics [interface *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows statistics for the specified interface.

Defaults

This command shows statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ip verify statistics** command:

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

show ips

To show all available IPS virtual sensors that are configured on the AIP SSM, use the **show ips** command in privileged EXEC mode.

show ips [**detail**]

Syntax Description

detail	(Optional) Shows the sensor ID number as well as the name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

In multiple context mode, this command shows all virtual sensors when entered in the system execution space, but only shows the virtual sensors assigned to the context in the context execution space. See the **allocate-ips** command to assign virtual sensors to contexts.

Virtual sensors are available in IPS Version 6.0 and above.

Examples

The following is sample output from the **show ips** command:

```
hostname# show ips
Sensor name
------------
ips1
ips2
```

The following is sample output from the **show ips detail** command:

```
hostname# show ips detail
Sensor name              Sensor ID
------------             ---------
ips1                     1
ips2                     2
```

Related Commands

Command	Description
allocate-ips	Assigns a virtual sensor to a security context.
ips	Diverts traffic to the AIP SSM.

show ipsec sa

To display a list of IPSec SAs, use the **show ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec sa**.

show ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPSec SAs sorted by peer address
identity	(Optional) Displays IPSec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPSec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPSec SAs for specified peer IP addresses.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPSec SA policy states that fragmentation occurs before IPSec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPSec processing.

The following example, entered in global configuration mode, displays IPSec SAs for a crypto map named def.

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
```

```
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 480
        IV size: 8 bytes
        replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
        transform: esp-3des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 4, crypto-map: def
        sa timing: remaining key lifetime (sec): 263
        IV size: 8 bytes
        replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
```

```
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example shows IPSec SAs with the keyword **identity**.

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPSec SAs with the keywords **identity** and **detail**.

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPSec SAs, use the **show ipsec sa summary** command in global configuration mode or privileged EXEC mode.

show ipsec sa summary

Syntax Description

This command has no arguments or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, displays a summary of IPSec SAs by the following connection types:

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN load balancing

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:           Peak IPSec SA's:
IPSec            :     2        Peak Concurrent SA  :    14
IPSec over UDP   :     2        Peak Concurrent L2L :     0
IPSec over NAT-T :     4        Peak Concurrent RA  :    14
IPSec over TCP   :     6
IPSec VPN LB     :     0
Total            :    14
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Removes IPSec SAs entirely or based on specific parameters.
show ipsec sa	Displays a list of IPSec SAs.
show ipsec stats	Displays a list of IPSec statistics.

show ipsec stats

To display a list of IPSec statistics, use the **show ipsec stats** command in global configuration mode or privileged EXEC mode.

show ipsec stats

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, displays IPSec statistics:

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
```

```
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Clears IPSec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPSec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPSec SAs.

show ipv6 access-list

To display the IPv6 access list, use the **show ipv6 access-list** command in privileged EXEC mode. The IPv6 access list determines what IPv6 traffic can pass through the security appliance.

show ipv6 access-list [*id* [*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*]]

Syntax Description

any	(Optional) An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	(Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed.
id	(Optional) The access list name. When provided, only the specified access list is displayed.
source-ipv6-prefix /*prefix-length*	(Optional) IPv6 network address and prefix. When provided, only the access rules for the specified IPv6 network are displayed.

Defaults

Displays all IPv6 access lists.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 access-list** command. It shows IPv6 access lists named inbound, tcptraffic, and outbound.

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
```

```
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

Related Commands

Command	Description
ipv6 access-list	Creates an IPv6 access list.

show ipv6 interface

To display the status of interfaces configured for IPv6, use the **show ipv6 interface** command in privileged EXEC mode.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

Syntax Description

brief	Displays a brief summary of IPv6 status and configuration for each interface.
if_name	(Optional) The internal or external interface name, as designated by the **nameif** command. The status and configuration for only the designated interface is shown.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool.

Defaults

Displays all IPv6 interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show interface** command, except that it is IPv6-specific. If the interface hardware is usable, the interface is marked *up*. If the interface can provide two-way communication, the line protocol is marked *up*.

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 interface** command:

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
```

```
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

The following is sample output from the **show ipv6 interface** command. It shows the characteristics of an interface which has generated a prefix from an address.

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counter information, use the **show ipv6 mld traffic** command in privileged EXEC mode.

show ipv6 mld traffic

Syntax Description

This command has no keywords or variables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

The **show ipv6 mld traffic** command allows you to check if the expected number of MLD messages have been received and sent.

The following information is provided by the **show ipv6 mld traffic** command:

- **Elapsed time since counters cleared**—the amount of time since the counters were cleared.
- **Valid MLD Packets**—the number of valid MLD packets that are received and sent.
- **Queries**—the number of valid queries that are received and sent.
- **Reports**—the number of valid reports that are received and sent.
- **Leaves**—the number of valid leaves received and sent.
- **Mtraee packets**—the number of multicast trace packets that are received and sent.
- **Errors**—the types of errors and the numberof errors that have occurred.

Examples

The following is sample output from the **show ipv6 mld traffic** command:

```
hostname# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                   Received           Sent
Valid MLD Packets  1                  3
```

```
Queries            1                   0
Reports            0                   3
Leaves             0                   0
Mtrace packets     0              0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

Command	Description
clear ipv6 mld traffic	Resets all MLD traffic counters.

show ipv6 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command in privileged EXEC mode.

show ipv6 neighbor [*if_name* | *address*]

Syntax Description

address	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
if_name	(Optional) Displays cache information for the supplied interface name, as configure by the **nameif** command, only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The following information is provided by the **show ipv6 neighbor** command:

- **IPv6 Address**—the IPv6 address of the neighbor or interface.
- **Age**—the time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- **Link-layer Addr**—MAC address. If the address is unknown, a hyphen (-) is displayed.
- **State**—The state of the neighbor cache entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the **INCMP** (Incomplete) and **REACH** (Reachable) states are different for dynamic and static cache entries.

The following are possible states for dynamic entries in the IPv6 neighbor discovery cache:

- **INCMP**—(Incomplete) Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

  - **REACH**—(Reachable) Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in **REACH** state, the device takes no special action as packets are sent.
  - **STALE**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in **STALE** state, the device takes no action until a packet is sent.
  - **DELAY**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the **DELAY** state, send a neighbor solicitation message and change the state to **PROBE**.
  - **PROBE**—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
  - **????**—Unknown state.

  The following are possible states for static entries in the IPv6 neighbor discovery cache:

  - **INCMP**—(Incomplete) The interface for this entry is down.
  - **REACH**—(Reachable) The interface for this entry is up.

- **Interface**
  Interface from which the address was reachable.

Examples

The following is sample output from the **show ipv6 neighbor** command when entered with an interface:

```
hostname# show ipv6 neighbor inside
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                  0 0003.a0d6.141e  REACH inside
3001:1::45a                               - 0002.7d1a.9472  REACH inside
```

The following is sample output from the **show ipv6 neighbor** command when entered with an IPv6 address:

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                            Age Link-layer Addr State Interface
2000:0:0:4::2                             0 0003.a0d6.141e  REACH inside
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.

show ipv6 route

To display the contents of the IPv6 routing table, use the **show ipv6 route** command in privileged EXEC mode.

show ipv6 route

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show route** command, except that the information is IPv6-specific.

The following information appears in the IPv6 routing table:

- **Codes**—Indicates the protocol that derived the route. Values are as follows:
  - **C**—Connected
  - **L**—Local
  - **S**—Static
  - **R**—RIP derived
  - **B**—BGP derived
  - **I1**—ISIS L1—Integrated IS-IS Level 1 derived
  - **I2**—ISIS L2—Integrated IS-IS Level 2 derived
  - **IA**—ISIS interarea—Integrated IS-IS interarea derived
- **fe80::/10**—Indicates the IPv6 prefix of the remote network.
- **[0/0]**—The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
- **via ::**—Specifies the address of the next router to the remote network.

- **inside**—Specifies the interface through which the next router to the specified network can be reached.

Examples

The following is sample output from the **show ipv6 route** command:

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

Related Commands

Command	Description
debug ipv6 route	Displays debug messages for IPv6 routing table updates and route cache updates.
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 routers

To display IPv6 router advertisement information received from on-link routers, use the **show ipv6 routers** command in privileged EXEC mode.

show ipv6 routers [*if_name*]

Syntax Description

if_name	(Optional) The internal or external interface name, as designated by the **nameif** command, that you want to display information about.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an interface name:

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

Command	Description
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in privileged EXEC mode.

show ipv6 traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **clear ipv6 traffic** command to clear the traffic counters.

Examples

The following is sample output from the **show ipv6 traffic** command:

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

Related Commands

Command	Description
clear ipv6 traffic	Clears ipv6 traffic counters.

CHAPTER 27

show isakmp ipsec-over-tcp stats through show route Commands

show isakmp ipsec-over-tcp stats

To display runtime statistics for IPsec over TCP, use the **show isakmp ipsec-over tcp stats** command in global configuration mode or privileged EXEC mode.

show isakmp ipsec-over-tcp stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp ipsec-over-tcp stats** command was introduced.
7.2(1)	The **show isakmp ipsec-over-tcp stats** command was deprecated. The **show crypto isakmp ipsec-over-tcp stats** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures

- Checksum errors
- Internal errors

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show isakmp ipsec-over-tcp stats
Global IPSec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show isakmp sa

To display the IKE runtime SA database, use the **show isakmp sa** command in global configuration mode or privileged EXEC mode.

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
hostname(config)# show isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in global configuration mode or privileged EXEC mode.

show isakmp stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets

- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show kernel process

To display the current status of the active kernel processes running on the security appliance, use the **show kernel process** command in privileged EXEC mode.

show kernel process

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.0(0)	This command was introduced.

Usage Guidelines

Use the show kernel process command to troubleshoot issues with the kernel running on the security appliance.

The output from the show kernel process command is lined up in the console output.

Examples

The following example displays output from the show kernel process command:

```
hostname# show kernel process

PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
```

```
hostname#
```

Table 27-1shows each field description.

Table 27-1 show kernel process Fields

Field	Description
PID	The process ID.
PPID	The parent process ID.
PRI	The priority of the process.
NI	The nice value, which is used in priority computation. The values range from 19 (nicest) to -19 (not nice to others),
VSIZE	The virtual memory size in bytes.
RSS	The resident set size of the process, in kilobytes.
WCHAN	The channel in which the process is waiting.
STAT	The state of the process: • R—Running • S—Sleeping in an interruptible wait • D—Waiting in an uninterruptible disk sleep • Z—zombie • T—Traced or stopped (on a signal) • P—Paging
RUNTIME	The number of jiffies that the process has been scheduled in user mode and kernel mode. The runtime is the sum of utime and stime.
COMMAND	The process name.

show local-host

To display the network states of local hosts, use the **show local-host** command in privileged EXEC mode.

show local-host [*ip_address*] [**detail**] [**all**][**brief**] **[connection {tcp <start>[-<end>] | udp <start>[-<end>] | embryonic <start>[-<end>]}]**

Syntax Description

all	(Optional) Includes local hosts connecting to the security appliance and from the security appliance.
brief	(Optional) Displays brief informationon local hosts.
connection	(Optional) Displays three typs of filters based on the number and type of connetcions: tcp, udp and embryonic. These filters can be used individually or jointly.
detail	(Optional) Displays the detailed network states of local host information, including more information about active xlates and network connections.
ip_address	(Optional) Specifies the local host IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	For models with host limits, this command now shows which interface is considered to be the outside interface.
7.2(4)	Two new options, *connection* and *brief*, were added to the **show local-host** command so that the output is filtered by the number of connections for the inside hosts.

Usage Guidelines

The **show local-host** command lets you display the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the security appliance.

This command lets you show the translation and connection slots for the local hosts. This command provides information for hosts that are configured with the **nat 0 access-list** command when normal translation and connection states may not apply.

This command also displays the connection limit values. If a connection limit is not set, the value displays as 0 and the limit is not applied.

For models with host limits, In routed mode, hosts on the inside (Work and Home zones) count towards the limit only when they communicate with the outside (Internet zone). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Work and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit.

In the event of a SYN attack (with TCP intercept configured), the **show local-host** command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

In the **show local-host** command output, the `TCP embryonic count to host counter` is used when a maximum embryonic limit (TCP intercept watermark) is configured for a host using a static connection. This counter shows the total embryonic connections to the host from other hosts. If this total exceeds the maximum configured limit, TCP intercept is applied to new connections to the host.

Examples

The following sample output is displayed by the **show local-host** command:

```
hostname# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a security appliance with host limits:

```
hostname# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a security appliance with host limits, but without a default route, the host limits apply to all interfaces. The default route interface might not be detected if the default route or the interface that the route uses is down.

```
hostname# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

The following sample output is displayed by the **show local-host** command on a security appliance with unlimited hosts:

```
hostname# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

The following examples show how to display the network states of local hosts:

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
```

```
Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

The following example shows all hosts who have at least four udp connections and have between one to 10 tcp connections at the same time:

```
hostname# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
        watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
        Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
        10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
        10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
        10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
        maximum active, 0 denied
```

The following example shows local-host addresses and connection counters using the **brief** option:

```
hostname# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
        TCP flow count/limit = 1/unlimited
        TCP embryonic count to host = 0
        TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

The following examples shows the output when using the *brief* and *connection* syntax:

```
hostname#show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

hostname# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

Related Commands

Command	Description
clear local-host	Releases network connections from local hosts displayed by the **show local-host** command.
nat	Associates a network with a pool of global IP addresses.

show logging

To show the logs in the buffer or other logging settings, use the **show logging** command in privileged EXEC mode.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

Syntax Description

all	(Optional) Displays all system log message IDs, along with whether they are enabled or disabled.
asdm	(Optional) Displays ASDM logging buffer content.
message	(Optional) Displays messages that are at a non-default level. See the **logging message** command to set the message level.
queue	(Optional) Displays the system log message queue.
setting	(Optional) Displays the logging setting, without displaying the logging buffer.
syslog_id	(Optional) Specifies a message number to display.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.
8.0(2)	Indicates whether a syslog server is configured to use an SSL/TLS connection.
8.0(5)	Tries to reconnect each minute to a TCP or secure host server.

Usage Guidelines

If the **logging buffered** command is in use, the **show logging** command without any keywords shows the current message buffer and the current settings.

The **show logging queue** command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them

Note Zero is an acceptable number for the configured queue size, and represents the maximum queue size allowed. The output for the **show logging queue** command will display the actual queue size if the the configured queue size is zero.

Examples

The following example shows the output from the **show logging** command:

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

The following example shows the output from the **show logging** command with a secure syslog server configured:

```
hostname(config)# logging host inside 10.0.0.1 TCP/1500 secure
hostname(config)# show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
        Logging to management 10.65.71.31 tcp/7777 Connected
         Logging to management 10.76.11.35 tcp/2222 Not connected since Sat, 21 Feb 2009
23:30:09 UTC
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

The following example shows the output from the **show logging message all** command:

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

Related Commands

Command	Description
logging asdm	Enables logging to ASDM
logging buffered	Enables logging to the buffer.
logging host	Defines a syslog server.
logging message	Sets the message level, or disables messages.
logging queue	Configures the logging queue.

show logging rate-limit

To display the disallowed system log messages to the original set, use the **show logging rate-limit** command in privileged EXEC mode.

show logging rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

This example shows how to display the disallowed system log messages:

```
hostname(config)# show logging rate-limit
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.

show mac-address-table

To show the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

show mac-address-table [*interface_name* | **count** | **static**]

Syntax Description

count	(Optional) Lists the total number of dynamic and static entries.
interface_name	(Optional) Identifies the interface name for which you want to view MAC address table entries.
static	(Optional) Lists only static entries.

Defaults

If you do not specify an interface, all interface MAC address entries are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mac-address-table** command:

```
hostname# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table** command for the inside interface:

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table count** command:

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds a static MAC address entry to the MAC address table.
mac-learn	Disables MAC address learning.

show management-access

To display the name of the internal interface configured for management access, use the show management-access command in privileged EXEC mode.

show management-access

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface and display the result:

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the security appliance.
management-access	Configures an internal interface for management access.

show memory

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory** command in privileged EXEC mode.

show memory [**detail**]

Syntax Description

detail	(Optional) Displays a detailed view of free and allocated system memory.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show memory** command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

You can use the **show memory detail** output with **show memory binsize** command to debug memory leaks.

The **show memory detail** command output can be broken down into three sections: Summary, DMA Memory, and HEAP Memory. The summary displays how the total memory is allocated. Memory that is not tied to DMA or reserved is considered the HEAP. The memory labeled Free Memory is the unused memory in the HEAP. The Allocated memory in use value is how much of the HEAP has been allocated. The break down of HEAP allocation is displayed later in the output. Reserved memory and DMA Reserved memory are used by different system processes and primarily VPN services.

You can also display the information from the **show memory** command using SNMP.

Examples

This example shows how to display a summary of the maximum physical memory and current free memory available:

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

This example shows detailed memory output:

```
hostname# show memory detail
Free memory:                                130546920 bytes (49%)
Used memory:                                137888536 bytes (51%)
    Allocated memory in use:                 33030808 bytes (12%)
    Reserved memory:                         65454208 bytes (24%)
    DMA Reserved memory:                     39403520 bytes (15%)
    ----------------------------        ----------------
Total memory:                           268435456 bytes (100%)
Dynamic Shared Objects(DSO):                0 bytes
DMA memory:
    Unused memory:                      3212128 bytes ( 8%)
    Crypto reserved memory:             2646136 bytes ( 7%)
        Crypto free:                    1605536 bytes ( 4%)
        Crypto used:                    1040600 bytes ( 3%)
    Block reserved memory:              33366816 bytes (85%)
        Block free:                     31867488 bytes (81%)
        Block used:                     1499328 bytes ( 4%)
    Used memory:                         178440 bytes ( 0%)
    ----------------------------        ----------------
    Total memory:                       39403520 bytes (100%)
    HEAP memory:
        Free memory:                    130546920 bytes (80%)
        Used memory:                    33030808 bytes (20%)
            Init used memory by library:  4218752 bytes ( 3%)
            Allocated memory:           28812056 bytes (18%)
    ----------------------------        ----------------
    Total memory:                       163577728 bytes (100%)

Least free memory:     122963528 bytes (75%)
Most used memory:      40614200 bytes (25%)

    ----- fragmented memory statistics -----

fragment size      count       total
    (bytes)                   (bytes)
---------------- ---------- --------------
        16         113         1808

<--- More --->
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory app-cache

To display real-time statistics for the application cache data structure that is used by many key applications including the data path on the system use the **show memory app-cache** command in privileged EXEC mode.

show memory app-cache [threat-detection | host | flow | tcb] [detail]

Syntax Description

flow	(Optional) Shows application level memory cache for flow.
host	(Optional) Show application level memory cache for host.
tcb	(Optional) Show application level memory cache for tcb.
threat-detection	(Optional) Show application level memory cache for threat-detetcion.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(1)	This command was introduced.

Usage Guidelines

The information displayed by the **show memory app-cache** command is useful for monitoring the app-cache operation, troubleshooting memory leak, and analyzing the system's traffic load distribution on a multi-core system.

Examples

This example shows the **show memory app-cache** command output:

```
hostname(config)# sh mem app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn chunk 700 0 24175 0 15181900
SNP Host Container 700 0 48330 0 6766200
SNP conn set counte 700 0 0 0 0
SNP APP ID chunk 700 0 0 0 0
SNP Run-time Inspec 700 0 0 0 0
SNP TCB chunk 700 0 36328 0 6539040
SNP MP PF Mod chunk 700 0 0 0 0
SNP MP SVC Conn chu 700 0 0 0 0
SNP SVC Session chu 700 0 0 0 0
SNP Midpath Service 700 0 0 0 0
SNP MP Stack chunk 700 0 1 0 364
CP APP ID chunk 700 0 0 0 0
SNP ACE statistics 50 0 0 0 0
SNP Host statistics 50 0 3732 0 26586768
SNP Subnet statisti 50 0 1796 0 3146592

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8550 0 114449 0 58220864

hostname(config)# sh mem app-cache threat-detection d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP ACE statistics 50 0 0 0 0
SNP Host statistics 50 50 50 0 356200
SNP Subnet statisti 50 50 50 0 87600

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 150 100 100 0 443800

hostname(config)# sh mem app-cache host d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Container 700 700 700 0 98000

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 98000

hostname(config)# sh mem app-cache flow d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn chunk 700 700 700 0 439600

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 439600

hostname(config)# sh mem app-cache tcb d
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB chunk 700 700 700 0 126000

LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 700 700 700 0 126000
```

Related Commands

Command	Description
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.
show memory-caller address	Displays the address ranges configured on the security appliance.

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory binsize

To display summary information about the chunks allocated for a specific bin size, use the **show memory binsize** command in privileged EXEC mode.

show memory binsize *size*

Syntax Description

size	Displays chunks (memory blocks) of a specific bin size. The bin size is from the "fragment size" column of the **show memory detail** command output.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example displays summary information about a chunk allocated to a bin size of 500:

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

Related Commands

Command	Description
show memory-caller address	Displays the address ranges configured on the security appliance.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory delayed-free-poisoner

To display a summary of the **memory delayed-free-poisoner** queue usage, use the **show memory delayed-free-poisoner** command in privileged EXEC mode.

show memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **clear memory delayed-free-poisoner** command to clear the queue and statistics.

Examples

This following is sample output from the **show memory delayed-free-poisoner** command:

```
hostname# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
         3335600:  memory held in queue
            6095:  current queue count
               0:  elements dequeued
               3:  frees ignored by size
            1530:  frees ignored by locking
              27:  successful validate runs
               0:  aborted validate runs
        01:09:36:  local time of last validate
```

Table 27-2 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 27-2 **show memory delayed-free-poisoner** Command Output Descriptions

Field	Description
memory held in queue	The memory that is held in the delayed free-memory poisoner tool queue. Such memory is normally in the "Free" quantity in the **show memory** output if the delayed free-memory poisoner tool is not enabled.
current queue count	The number of elements in the queue.
elements dequeued	The number of elements that have been removed from the queue. This number begins to increase when most or all of the otherwise free memory in the system ends up in being held in the queue.
frees ignored by size	The number of free requests not placed into the queue because the request was too small to hold required tracking information.
frees ignored by locking	The number of free requests intercepted by the tool not placed into the queue because the memory is in use by more than one application. The last application to free the memory back to the system ends up placing such memory regions into the queue.
successful validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that the queue contents were validated (either automatically or by the **memory delayed-free-poisoner validate** command).
aborted validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that requests to check the queue contents have been aborted because more than one task (either the periodic run or a validate request from the CLI) attempted to use the queue at a time.
local time of last validate	The local system time when the last validate run completed.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.

show memory profile

To display information about the memory usage (profiling) of the security appliance, use the **show memory profile** command in privileged EXEC mode.

show memory profile [peak] [**detail** | **collated | status**]

Syntax Description

collated	(Optional) Collates the memory information displayed.
detail	(Optional) Displays detailed memory information.
peak	(Optional) Displays the peak capture buffer rather than the “in use” buffer.
status	(Optional) Displays the current state of memory profiling and the peak capture buffer**.**

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **show memory profile** command to troubleshoot memory usage level and memory leaks. You can still see the profile buffer contents even if profiling has been stopped. Starting profiling clears the buffer automatically.

Note The security appliance might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows...

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

The output of the **show memory profile detail** command (below) is divided into six data columns and one header column, at the far left. The address of the memory bucket corresponding to the first data column is given at the header column (the hexidecimal number). The data itself is the number of bytes

that is held by the text/code that falls in the bucket address. A period (.) in the data column means no memory is held by the text at this bucket. Other columns in the row correspond to the bucket address that is greater than the increment amount from the previous column. For example, the address bucket of the first data column in the first row is 0x001069e0. The address bucket of the second data column in the first row is 0x001069e4 and so on. Normally the header column address is the next bucket address; that is, the address of the last data column of the previous row plus the increment. All rows without any usage are suppressed. More than one such contiguous row can be suppressed, indicated with three periods at the header column (...).

```
hostname# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

The following example shows collated output:

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<snip>
```

The following example shows the peak capture buffer:

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

The following example shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

The following example shows the current state of memory profiling and the peak capture buffer:

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a program text range of memory to profile.
clear memory profile	Clears the memory buffers held by the memory profiling function.

show memory tracking

To display currently allocated memory tracked by the tool, use the show memory tracking command in privileged EXEC mode.

show memory tracking [address | dump | detail]

Syntax Description

address	(Optional) Shows memory tracking by address.
detail	(Optional) Shows internal memory tracking state.
dump	(Optional) Dumps memory tracking address.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

Use the **show memory tracking** command to show currently allocated memory tracked by the tool.

Examples

The following example shows the **show memory tracking** command out-put:

```
hostname# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

The following examples show the **show memory tracking address**, and **show memory tracking dump** outputs:

```
hostname# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

```
memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2

hostname# memory tracking dump 0xa893aed0
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

Related Commands

Command	Description
clear memory tracking	Clears all currently gathered information.
show memory tracking	Shows currently allocated memory.

show memory webvpn

To generate memory usage statistics for webvpn, use the **show memory webvpn** command in privileged EXEC mode.

show memory webvpn [allobjects | blocks | dumpstate [cache | disk0 | disk1 | flash | ftp | system | tftp]| pools | profile [clear | dump | start | stop] | usedobjects {{begin | exclude | grep | include} line *line***}]**

Syntax Description

allobjects	Displays webvpn memory consumption details for pools, blocks and all used and freed objects.
begin	Begins with the line that matches.
blocks	Displays webvpn memory consumption details for memory blocks.
cache	Specifies a filename for a webvpn memory cache state dump.
clear	Clears the webvpn memory profile.
disk0	Specifies a filename for webvpn memory disk0 state dump.
disk1	Specifies a filename for webvpn memory disk1 state dump:.
dump	Puts webvpn memory profile into a file.
dumpstate	Puts webvpn memory state into a file.
exclude	Excludes the line(s) that match.
flash	Specifies a filename for webvpn memory flash state dump.
ftp	Specifies a filename for webvpn memory ftp state dump.
grep	Includes/excludes lines that match.
include	Includes the line(s) that match.
line	Identifies the line(s) to match.
line	Specifies the line(s) to match.
pools	Show webvpn memory consumption details for memory pools.
profile	Gathers the webvpn memory profile and places it in a file.
system	Specifies a filename for webvpn memory system state dump.
start	Starts gathering the webvpn memory profile.
stop	Stops gathering the webvpn memory profile.
tftp	Specifies a filename for a webvpn memory tftp state dump.
usedobjects	Displays webvpn memory consumption details for used objects.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following is sample output from the **show memory webvpn allobjects** command:

```
hostname# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

Related Commands

Command	Description
memory-size	Sets the amount of memory on the security appliance that WebVPN services can use.

show memory-caller address

To display the address ranges configured on the security appliance, use the **show memory-caller address** command in privileged EXEC mode.

show memory-caller address

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first configure an address ranges with the **memory caller-address** command before you can display them with the **show memory-caller address** command.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

If address ranges are not configured before entering the **show memory-caller address** command, no addresses display:

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

Related Commands

Command	Description
memory caller-address	Configures block of memory for the caller PC.

show mfib

To display MFIB in terms of forwarding entries and interfaces, use the **show mfib** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] [**verbose**]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.
verbose	(Optional) Displays additional information about the entries.

Defaults

Without the optional arguments, information for all groups is shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib** command:

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib verbose	Displays detail information about the forwarding entries and interfaces.

show mfib active

To display active multicast sources, use the **show mfib active** command in user EXEC or privileged EXEC mode.

show mfib [*group*] **active** [*kbps*]

Syntax Description

group	(Optional) IP address of the multicast group.
kbps	(Optional) Limits the display to multicast streams that are greater-than or equal to this value.

This command has no arguments or keywords.

Defaults

The default value for *kbps* is 4. If a *group* is not specified, all groups are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The output for the show mfib active command displays either positive or negative numbers for the rate PPS. The security appliance displays negative numbers when RPF packets fail or when the router observes RPF packets with an interfaces out (OIF) list. This type of activity may indicate a multicast routing problem.

Examples

The following is sample output from the **show mfib active** command:

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
```

```
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Related Commands

Command	Description
show mroute active	Displays active multicast streams.

show mfib count

To display MFIB route and packet count data, use the **show mfib count** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] **count**

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays packet drop statistics.

Examples

The following sample output from the **show mfib count** command:

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

Related Commands

Command	Description
clear mfib counters	Clears MFIB router packet counters.
show mroute count	Displays multicast route counters.

show mfib interface

To display packet statistics for interfaces that are related to the MFIB process, use the **show mfib interface** command in user EXEC or privileged EXEC mode.

show mfib interface [*interface*]

Syntax Description

interface	(Optional) Interface name. Limits the display to the specified interface.

Defaults

Information for all MFIB interfaces is shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example is sample output from the **show mfib interface** command:

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                             [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib reserved

To display reserved groups, use the **show mfib reserved** command in user EXEC or privileged EXEC mode.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

Syntax Description

count	(Optional) Displays packet and route count data.
verbose	(Optional) Displays additional information.
active	(Optional) Displays active multicast sources.
kpbs	(Optional) Limits the display to active multicast sources greater-than or equal to this value.

Defaults

The default value for *kbps* is 4.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays MFIB entries in the range 224.0.0.0 through 224.0.0.225.

Examples

The following is sample output from the **show mfib reserved** command:

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
```

```
dmz Flags: IC
inside Flags: IC
```

Related Commands

Command	Description
show mfib active	Displays active multicast streams.

show mfib status

To display the general MFIB configuration and operational status, use the **show mfib status** command in user EXEC or privileged EXEC mode.

show mfib status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib status** command:

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib summary

To display summary information about the number of MFIB entries and interfaces, use the **show mfib summary** command in user EXEC or privileged EXEC mode.

show mfib summary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib summary** command:

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

Related Commands

Command	Description
show mroute summary	Displays multicast routing table summary information.

show mfib verbose

To display detail information about the forwarding entries and interfaces, use the **show mfib verbose** command in user EXEC or privileged EXEC mode.

show mfib verbose

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mfib verbose** command:

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.
show mfib summary	Displays summary information about the number of MFIB entries and interfaces.

show mgcp

To display MGCP configuration and session information, use the **show mgcp** command in privileged EXEC mode.

show mgcp {**commands** | **sessions**} [**detail**]

Syntax Description

commands	Lists the number of MGCP commands in the command queue.
sessions	Lists the number of existing MGCP sessions.
detail	(Optional) Lists additional information about each command (or session) in the output.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show mgcp commands** command lists the number of MGCP commands in the command queue. The **show mgcp sessions** command lists the number of existing MGCP sessions. The **detail** option includes additional information about each command (or session) in the output.

Examples

The following are examples of the **show mgcp** command options:

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
hostname#

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
```

```
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058
hostname#

hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
hostname#

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
hostname#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.

show mmp

To display information about existing MMP sessions, use the **show mmp** command in privileged EXEC mode.

show mmp [*address*]

Syntax Description

address	Specifies the IP address of an MMP client/server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **show mmp** command to display information about existing MMP sessions:

```
hostname# show mmp 10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

Related Commands

Command	Description
debug mmp	Displays inspect MMP events.
inspect mmp	Configures the MMP inspection engine.
show debug mmp	Displays current debug settings for the MMP inspection module.

show mode

To show the security context mode for the running software image and for any image in Flash memory, use the **show mode** command in privileged EXEC mode.

show mode

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show mode** command. The following example shows the current mode and the mode for the non-running image “image.bin”:

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

The mode can be multiple or single.

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
mode	Sets the context mode to single or multiple.

show module

To show information about the SSM on the ASA 5500 series adaptive security appliance as well as system information, use the **show module** command in user EXEC mode.

show module [**all** | *slot* [**details** | **recover**]]

Syntax Description

all	(Default) Shows information for the SSM in slot 1 and the system in slot 0.
details	(Optional) Shows additional information, including remote management configuration for intelligent SSMs (for example, ASA-SSM-*x*0).
recover	(Optional) For intelligent SSMs, shows the settings for the **hw-module module recover** command. **Note** The **recover** keyword is valid only when you have created a recovery configuration for the SSM by using the **configure** keyword with the **hw-module module recover** command.
slot	(Optional) Specifies the slot number, 0 or 1. Slot 0 is the security appliance base system.

Defaults

The information appears for both slots.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context[1]	System
User EXEC	•	•	•	•	•

1. The **show module recover** command is only available in the system execution space.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was modified to include more detail in the output.

Usage Guidelines

This command shows information about the SSM as well as the system and built-in interfaces.

Examples

The following is sample output from the **show module** command. Slot 0 is the base system, while slot 1 is a CSC SSM.

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
```

```
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

Table 22 shows each field description.

Table 27-3 show module Fields

Field	Description
Mod	The slot number, 0 or 1.
Card Type	For the system shown in slot 0, the type is the platform model. For the SSM in slot 1, the type is the SSM type.
Model	The model for this slot.
Serial No.	The serial number.
MAC Address Range	The MAC address range for interfaces on this SSM or, for the system, the built-in interfaces.
Hw Version	The hardware version.
Fw Version	The firmware version.
Sw Version	The software version.
SSM Application Name	The name of the application running on the SSM.
SSM Application Version	The version of the application running on the SSM.
Status	For the system in slot 0, the status is Up Sys. The status of the SSM in slot 1 can be any of the following: • Initializing—The SSM is being detected and the control communication is being initialized by the system. • Up—The SSM has completed initialization by the system. • Unresponsive—The system encountered an error while communicating with this SSM. • Reloading—For intelligent SSMs, the SSM is reloading. • Shutting Down—The SSM is shutting down. • Down—The SSM is shut down. • Recover—For intelligent SSMs, the SSM is attempting to download a recovery image.

Table 27-3 show module Fields (continued)

Field	Description
Data Plane Status	The current state of the data plane to the SSM.
Compatibility	The compatibility of the SSM relative to the rest of the system.

The output of the **show module details** command varies dependingpon which SSM is in the slot. For example, output for the CSC SSM includes fields about components of the CSC SSM software. These fields do not appear if the slot has an AIP SSM instead. The following is generic sample output from the **show module details** command:

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

Table 23 shows each field description. See Table 22 for fields that are also shown for the **show module** command.

Table 27-4 show module details Fields

Field	Description
Mgmt IP addr	For intelligent SSMs, shows the IP address for the SSM management interface.
Mgmt web ports	For intelligent SSMs, shows the ports configured for the management interface.
Mgmt TLS enabled	For intelligent SSMs, shows whether transport layer security is enabled (true or false) for connections to the management interface of the SSM.

The following is sample output from the **show module** command when the **recover** keyword is used:

```
hostname> show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:          tftp://10.21.18.1/ids-oldimg
Port IP Address:    10.1.2.10
Port Mask :         255.255.255.0
Gateway IP Address: 10.1.2.254
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.

show mrib client

To display information about the MRIB client connections, use the **show mrib client** command in user EXEC or privileged EXEC mode.

show mrib client [**filter**] [**name** *client_name*]

Syntax Description

filter	(Optional) Displays client filter. Used to view information about the MRIB flags that each client owns and the flags in which each clients is interested.
name *client_name*	(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as PIM or IGMP.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **filter** option is used to display the route and interface level flag changes that various MRIB clients have registered. This command option also shows what flags are owned by the MRIB clients.

Examples

The following sample output from the **show mrib client** command using the **filter** keyword:

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
```

```
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

Command	Description
show mrib route	Displays MRIB table entries.

show mrib route

To display entries in the MRIB table, use the **show mrib route** command in user EXEC or privileged EXEC mode.

show mrib route [[*source* | *****] [*group*[*/prefix-length*]]]

Syntax Description

*****	(Optional) Display shared tree entries.
/prefix-length	(Optional) Prefix length of the MRIB route. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group	(Optional) IP address or name of the group.
source	(Optional) IP address or name of the route source.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets.

In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry. The **show mfib count** command displays global counters independent of the routes.

Examples

The following is sample output from the **show mrib route** command:

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
```

```
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

Command	Description
show mfib count	Displays route and packet count data for the MFIB table.
show mrib route summary	Displays a summary of the MRIB table entries.

show mroute

To display the IPv4 multicast routing table, use the **show mroute** command in privileged EXEC mode.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	(Optional) Displays only active multicast sources. Active sources are those sending at the specified *rate* or higher. If the *rate* is not specified, active sources are those sending at a rate of 4 kbps or higher.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
group	(Optional) IP address or name of the multicast group as defined in the DNS hosts table.
pruned	(Optional) Displays pruned routes.
reserved	(Optional) Displays reserved groups.
source	(Optional) Source hostname or IP address.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the multicast routing table.

Defaults

If not specified, the *rate* argument defaults to 4 kbps.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show mroute** command displays the contents of the multicast routing table. The security appliance populates the multicast routing table by creating (S,G) and (*,G) entries based on PIM protocol messages, IGMP reports, and traffic. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (through RPF).

To view the **mroute** commands in the running configuration, use the **show running-config mroute** command.

Examples

The following is sample output from the **show mroute** command:

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

The following fields are shown in the **show mroute** output:

- **Flags**—Provides information about the entry.
  - **D—Dense**. Entry is operating in dense mode.
  - **S—Sparse**. Entry is operating in sparse mode.
  - **B—Bidir Group**. Indicates that a multicast group is operating in bidirectional mode.
  - **s—SSM Group**. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
  - **C—Connected**. A member of the multicast group is present on the directly connected interface.
  - **L—Local**. The security appliance itself is a member of the multicast group. Groups are joined locally by the **igmp join-group** command (for the configured group).
  - **I—Received Source Specific Host Report**. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMP. This flag is set only on the DR.
  - **P—Pruned**. Route has been pruned. The software keeps this information so that a downstream member can join the source.
  - **R—RP-bit set**. Indicates that the (S, G) entry is pointing toward the RP.
  - **F—Register flag**. Indicates that the software is registering for a multicast source.
  - **T—SPT-bit set**. Indicates that packets have been received on the shortest path source tree.
  - **J—Join SPT**. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the security appliance to join the source tree.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the security appliance monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

Note The security appliance measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the security appliance immediately switches to the shortest path source tree when traffic from a new source is received.

- **Timers:Uptime/Expires**—Uptime indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Expires indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
- **Interface state**—Indicates the state of the incoming or outgoing interface.
  - **Interface**—The interface name listed in the incoming or outgoing interface list.
  - **State**—Indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold.
- **(*, 239.1.1.40)** and **(* , 239.2.2.1)**—Entries in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source indicates all sources.
- **RP**—Address of the RP. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
- **Incoming interface**—Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
- **RPF nbr**—IP address of the upstream router to the source.
- **Outgoing interface list**—Interfaces through which packets will be forwarded.

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the running configuration.
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays configured multicast routes.

show nac-policy

To show the NAC policy usage statistics and the assignment of NAC policies to group policies, use the **show nac-policy** command in privileged EXEC mode.

show nac-policy [*nac-policy-name***]**

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to display usage statistics.

Defaults

If you do not specify a name, the CLI lists all NAC policy names along with their respective statistics.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows the data for the NAC policies named framework1 and framework2:

```
asa2(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

The first line of each NAC policy indicates its name and type (nac-framework). The CLI shows the text “is not in use” next to the policy type if the policy is not assigned to any group policies. Otherwise, the CLI displays the usage data for the group policy. Table 27-5 explains the fields in the **show nac-policy** command.

Table 27-5 show nac-policy Command Fields

Field	Description
applied session count	Cumulative number of VPN sessions to which this security appliance applied the NAC policy.

Table 27-5 show nac-policy Command Fields

Field	Description
applied group-policy count	Cumulative number of group polices to which this security appliance applied the NAC policy.
group-policy list	List of group policies to which this NAC policy is assigned. In this case, the usage of a group policy does not determine whether it appears in this list; if the NAC policy is assigned to a group policy in the running configuration, then the group policy appears in this list.

Related Commands

clear nac-policy	Resets the NAC policy usage statistics.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number IPSec, Cisco WebVPN, and NAC sessions.

show nameif

To view the interface name set using the **nameif** command, use the show nameif command in privileged EXEC mode.

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows all interface names.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context. The output for this command shows only the mapped name in the Interface column.

Examples

The following is sample output from the **show nameif** command:

```
hostname# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show nat

To display NAT policy counters, use the **show nat** command in privileged EXEC mode.

show nat *src_ifc* [*src_ip* [*src_mask*]] [*dst_ifc* [*dst_ip* [*dst_mask*]]]]

Syntax Description

dst_ifc	(Optional) Specifies destination interface to filter.
dst_ip	(Optional) Specifies destination IP address to filter.
dst_mask	(Optional) Specifies mask for destination IP address.
src_ifc	(Optional) Specifies source interface to filter.
src_ip	(Optional) Specifies source IP address to filter.
src_mask	(Optional) Specifies mask for source IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

When a **static**, **nat**, or **alias** command is configured, it is internally converted into NAT policies between applicable interfaces. The **show nat** command displays the policies that are looked up when translations or untranslations are performed.

The NAT policy output consists of the following information:

- The match clause for the traffic that should be matched
- The action to be taken after a match, which could be any of the following:
  - static translation
  - alias translation
  - identity NAT
  - NAT exempt
  - implicit deny because no translation group was found
- counters—translate_hits provide counters for real to mapped address conversion and untranslate_hits provide counters for mapped to real address conversion.

Examples

The following is sample output from the **show nat** command:

```
hostname(config)# show nat

NAT policies on Interface inside:
  match ip inside host 172.16.1.1 outside any
    static translation to 209.165.200.224
    translate_hits = 0, untranslate_hits = 0

NAT policies on Interface management:
  match ip management any outside 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any test 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any management 10.1.1.0 255.255.255.224
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip management any outside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any inside any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any test any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
  match ip management any management any
    identity NAT translation, pool 0
    translate_hits = 0, untranslate_hits = 0
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
nat-control	Enables/disables NAT configuration requirement.
nat-rewrite	Enables NAT rewrite for IP addresses embedded in the A-record of a DNS response.

show ntp associations

To view NTP association information, use the **show ntp associations** command in user EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows additional details about each association.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
User EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ntp associations** command:

```
hostname> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 27-6 shows each field description.

Table 27-6 show ntp associations Fields

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: • * —Synchronized to this peer. • # —Almost synchronized to this peer. • + —Peer selected for possible synchronization. • - —Peer is a candidate for selection. • ~ —Peer is statically configured, but not synchronized.
address	The address of the NTP peer.
ref clock	The address of the reference clock of the peer.
st	The stratum of the peer.
when	The time since the last NTP packet was received from the peer.
poll	The polling interval (in seconds).
reach	The peer reachability (as a bit string, in octal).
delay	The round-trip delay to the peer (in milliseconds).
offset	The relative time of the peer clock to the local clock (in milliseconds).
disp	The dispersion value.

The following is sample output from the **show ntp associations detail** command:

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62   16000.0
```

Table 27-7 shows each field description.

Table 27-7 show ntp associations detail Fields

Field	Description
IP-address configured	The server (peer) IP address.
(status)	• our_master—The security appliance is synchronized to this peer. • selected—Peer is selected for possible synchronization. • candidate—Peer is a candidate for selection.

Table 27-7 show ntp associations detail Fields (continued)

Field	Description
(sanity)	• sane—The peer passes basic sanity checks. • insane—The peer fails basic sanity checks.
(validity)	• valid—The peer time is believed to be valid. • invalid—The peer time is believed to be invalid. • leap_add—The peer is signalling that a leap second will be added. • leap-sub—The peer is signalling that a leap second will be subtracted.
stratum	The stratum of the peer.
(reference peer)	unsynced—The peer is not synchronized to any other machine. ref ID—The address of the machine that the peer is synchronized to.
time	The last time stamp the peer received from its master.
our mode client	Our mode relative to the peer, which is always client.
peer mode server	The peer's mode relative to us, which is always server.
our poll intvl	Our poll interval to the peer.
peer poll intvl	The peer poll interval to us.
root delay	The delay along the path to the root (ultimate stratum 1 time source).
root disp	The dispersion of the path to the root.
reach	The peer reachability (as a bit string in octal).
sync dist	The peer synchronization distance.
delay	The round-trip delay to the peer.
offset	The offset of the peer clock relative to our clock.
dispersion	The dispersion of the peer clock.
precision	The precision of the peer clock (in hertz).
version	The NTP version number that the peer is using.
org time	The originate time stamp.
rcv time	The receive time stamp.
xmt time	The transmit time stamp.
filtdelay	The round-trip delay (in milliseconds) of each sample.
filtoffset	The clock offset (in milliseconds) of each sample.
filterror	The approximate error of each sample.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.

Command	Description
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show ntp status

To show the status of each NTP association, use the **show ntp status** command in user EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ntp status** command:

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

Table 27-8 shows each field description.

Table 27-8 show ntp status Fields

Field	Description
Clock	• synchronized—The security appliance is synchronized to an NTP server. • unsynchronized—The security appliance is not synchronized to an NTP server.
stratum	NTP stratum of this system.

Table 27-8 show ntp status Fields

Field	Description
reference	The address of the NTP server to which the security appliance is synchronized.
nominal freq	The nominal frequency of the system hardware clock.
actual freq	The measured frequency of the system hardware clock.
precision	The precision of the clock of this system (in hertz).
reference time	The reference time stamp.
clock offset	The offset of the system clock to the synchronized peer.
root delay	The total delay along the path to the root clock.
root dispersion	The dispersion of the root path.
peer dispersion	The dispersion of the synchronized peer.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the security appliance is associated.

show ospf

To display the general information about the OSPF routing processes, use the **show ospf** command in privileged EXEC mode.

show ospf [*pid* **[***area_id***]**]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.

Defaults

Lists all OSPF processes if no *pid* is specified.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the *pid* is included, only information for the specified routing process is included.

Examples

The following is sample output from the **show ospf** command, showing how to display general information about a specific OSPF routing process:

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

The following is sample output from the **show ospf** command, showing how to display general information about all OSPF routing processes:

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
```

```
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the **show ospf border-routers** command in privileged EXEC mode.

show ospf border-routers

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the show **ospf border-routers** command:

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf database

To display the information contained in the OSPF topological database on the security appliance, use the **show ospf database** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originat**e | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

Syntax Description

addr	(Optional) Router address.
adv-router	(Optional) Advertised router.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
asbr-summary	(Optional) Displays an ASBR list summary.
database	Displays the database information.
database-summary	(Optional) Displays the complete database summary list.
external	(Optional) Displays routes external to a specified autonomous system.
internal	(Optional) Routes that are internal to a specified autonomous system.
lsid	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
pid	(Optional) ID of the OSPF process.
router	(Optional) Displays the router.
self-originate	(Optional) Displays the information for the specified autonomous system.
summary	(Optional) Displays a summary of the list.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf database** command:

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

The following is sample output from the **show ospf database asbr-summary** command:

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database router** command:

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
```

```
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following is sample output from the **show ospf database network** command:

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

The following is sample output from the **show ospf database summary** command:

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database external** command:

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf flood-list

To display a list of OSPF LSAs waiting to be flooded over an interface, use the **show ospf flood-list** command in privileged EXEC mode.

show ospf flood-list *interface_name*

Syntax Description

interface_name	The name of the interface for which to display neighbor information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf flood-list** command:

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf interface

To display the OSPF-related interface information, use the **show ospf interface** command in privileged EXEC mode.

show ospf interface [*interface_name*]

Syntax Description

interface_name	(Optional) Name of the interface for which to display the OSPF-related information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When used without the *interface_name* argument, the OSPF information for all interfaces is shown.

Examples

The following is sample output from the **show ospf interface** command:

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

Related Commands

Command	Description
interface	Opens interface configuration mode.

show ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the **show ospf neighbor** command in privileged EXEC mode.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

Syntax Description

detail	(Optional) Lists detail information for the specified router.
interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) Router ID of the neighbor router.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf neighbor** command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
neighbor	Configures OSPF routers interconnecting to non-broadcast networks.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf request-list

To display a list of all LSAs that are requested by a router, use the **show ospf request-list** command in privileged EXEC mode.

show ospf request-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.
nbr_router_id	Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf request-list** command:

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

Command	Description
show ospf retransmission-list	Displays a list of all LSAs waiting to be resent.

show ospf retransmission-list

To display a list of all LSAs waiting to be resent, use the **show ospf retransmission-list** command in privileged EXEC mode.

show ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.
nbr_router_id	Router ID of the neighbor router.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this interface.

Examples

The following is sample output from the **show ospf retransmission-list** command, where the *nbr_router_id* argument is 192.168.1.11 and the *if_name* argument is outside:

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

Command	Description
show ospf request-list	Displays a list of all LSAs that are requested by a router.

show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ospf summary-address** command in privileged EXEC mode.

show ospf summary-address

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following shows sample output from the **show ospf summary-address** command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

Related Commands

Command	Description
summary-address	Creates aggregate addresses for OSPF.

show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ospf virtual-links** command in privileged EXEC mode.

show ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show ospf virtual-links** command:

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

show perfmon

To display information about the performance of the security appliance, use the **show perfmon** command in privileged EXEC mode.

show perfmon [**detail**]

Syntax Description

detail	(Optional) Shows additional statsistics. These statistics match those gathered by the Global and Per-protocol connection objects of the Cisco Unified Firewall MIB.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the security appliance.
7.2(1)	The **detail** keyword was added.

Usage Guidelines

This command output does not display in a Telnet session.

The **perfmon** command shows performance statistics continuously at defined intervals. The **show perfmon** command allows you to display the information immediately.

Examples

The following is sample output for the **show perfmon** command:

```
hostname(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
```

```
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
```

The following is sample output for the **show perfmon detail** command:

```
hostname(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s           0/s
Connections          0/s           0/s
TCP Conns            0/s           0/s
UDP Conns            0/s           0/s
URL Access           0/s           0/s
URL Server Req       0/s           0/s
TCP Fixup            0/s           0/s
HTTP Fixup           0/s           0/s
FTP Fixup            0/s           0/s
AAA Authen           0/s           0/s
AAA Author           0/s           0/s
AAA Account          0/s           0/s
TCP Intercept        0/s           0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information at defined intervals.

show phone-proxy

To show phone-proxy specific information, use the **show phone-proxy** command in global configuration mode.

show phone-proxy [media-sessions [detail] | signaling-sessions [detai] | secure-phones]

Syntax Description

detail	Displays detailed information.
media-sessions	Displays the corresponding media sessions stored by the Phone Proxy.
secure-phones	Displays the phones capable of secure mode stored in the database.
signaling-sessions	Displays the corresponding signaling sessions stored by the Phone Proxy.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **show phone proxy** command to show Phone Proxy specific information:

```
hostname(config)# show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address     Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
hostname(config)#
```

The following example shows the use of the **show phone proxy** command to display the phones capable of secure mode stored in the database:

```
hostname(config)# show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used

Interface/IP Address      MAC               Timeout    Idle
------------------------  ----------        ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
hostname(config)#
```

The following example shows the use of the show phone proxy command to Show output from a successful call:

```
hostname(config)# show phone-proxy media-sessions
Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

Related Commands

Command	Description
debug phone-proxy	Displays debug messages for the Phone Proxy instance.
phone proxy	Configures the Phone Proxy instance.

show pim df

To display the bidirectional DF "winner" for a rendezvous point (RP) or interface, use the **show pim df** command in user EXEC or privileged EXEC mode.

show pim df [**winner**] [*rp_address* | *if_name*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.
if_name	The physical or logical interface name.
winner	(Optional) Displays the DF election winner per interface per RP.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

The following is sample output from the **show pim df** command:

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

To display group-to-protocol mapping table, use the **show pim group-map** command in user EXEC or privileged EXEC mode.

show pim group-map [**info-source**] [*group*]

Syntax Description

group	(Optional) Can be either one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
info-source	(Optional) Displays the group range information source.

Defaults

Displays group-to-protocol mappings for all groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the security appliance from different clients.

The PIM implementation on the security appliance has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

If multiple RPs are configured with the **pim rp-address** command, then the appropriate group range is displayed with their corresponding RPs.

Examples

The following is sample output form the **show pim group-map** command:

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info
```

```
224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.
pim rp-address	Configures the address of a PIM rendezvous point (RP).

show pim interface

To display interface-specific information for PIM, use the **show pim interface** command in user EXEC or privileged EXEC mode.

show pim interface [*if_name* | **state-off** | **state-on**]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
state-off	(Optional) Displays interfaces with PIM disabled.
state-on	(Optional) Displays interfaces with PIM enabled.

Defaults

If you do not specify an interface, PIM information for all interfaces is shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PIM implementation on the security appliance considers the security appliance itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

Examples

The following example displays PIM information for the inside interface:

```
hostname# show pim interface inside
Address     Interface      Ver/     Nbr     Query      DR     DR
                           Mode     Count   Intvl      Prior
172.16.1.4 inside          v2/S     2       100 ms     1      172.16.1.4
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in user EXEC or privileged EXEC mode.

show pim join-prune statistics [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the join/prune statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Clear the PIM join/prune statistics with the **clear pim counters** command.

Examples

The following is sample output from the **show pim join-prune statistic** command:

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

To display entries in the PIM neighbor table, use the **show pim neighbor** command in user EXEC or privileged EXEc mode.

show pim neighbor [**count** | **detail**] [*interface*]

Syntax Description

interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
count	(Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
detail	(Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The PIM implementation on the security appliance considers the security appliance itself to be a PIM neighbor. Therefore, the security appliance interface is shown in the output of this command. The IP address of the security appliance is indicated by an asterisk next to the address.

Examples

The following is sample output from the **show pim neighbor** command:

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in user EXEC or privileged EXEC mode.

show pim range-list [*rp_address*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

Examples

The following is sample output from the **show pim range-list** command:

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

Command	Description
show pim group-map	Displays group-to-PIM mode mapping and active RP information.

show pim topology

To display PIM topology table information, use the **show pim topology** command in user EXEC or privileged EXEC mode.

show pim topology [*group*] [*source*]

Syntax Description

group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
source	(Optional) Can be one of the following: • Name of the multicast source, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast source. This is a multicast IP address in four-part dotted-decimal notation.

Defaults

Topology information for all groups and sources is shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** command.

Examples

The following is sample output from the **show pim topology** command:

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

Related Commands

Command	Description
show mrib route	Displays the MRIB table.
show pim topology reserved	Displays PIM topology table information for reserved groups.

show pim topology reserved

To display PIM topology table information for reserved groups, use the **show pim topology reserved** command in user EXEC or privileged EXEC mode.

show pim topology reserved

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show pim topology reserved** command:

```
hostname# show pim topology reserved

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim topology route-count

To display PIM topology table entry counts, use the **show pim topology route-count** command in user EXEC or privileged EXEC mode.

show pim topology route-count [**detail**]

Syntax Description

detail	(Optional) Displays more detailed count information on a per-group basis.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command displays the count of entries in the PIM topology table. To display more information about the entries, use the **show pim topology** command.

Examples

The following is sample output from the **show pim topology route-count** command:

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim traffic

To display PIM traffic counters, use the **show pim traffic** command in user EXEC or privileged EXEC mode.

show pim traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Clear the PIM traffic counters with the **clear pim counters** command.

Examples

The following is sample output from the **show pim traffic** command:

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

To display information about the PIM tunnel interfaces, use the **show pim tunnel** command in user EXEC or privileged EXEC mode.

show pim tunnel [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the PIM tunnel information for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the RP. On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

Examples

The following is sample output from the **show pim tunnel** command:

```
hostname# show pim tunnel

Interface     RP Address Source Address

Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show power inline

For models with PoE interfaces, such as the ASA 5505 adaptive security appliance, use the **show power inline** command in user EXEC mode to show power status of the interfaces.

show power inline

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point.

Examples

The following is sample output from the **show power inline** command:

```
hostname> show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

Table 27-9 shows each field description:

Table 27-9 show power inline Fields

Field	Description
Interface	Shows all interfaces on the security appliance, including ones that do not have PoE available.
Power	Shows whether the power is On or Off. If a device does not need power, if there is no device on that interface, or if the interface is shut down the value is Off. If the interface does not support PoE, then the value is n/a.
Device	Shows the type of device obtaining power, either Cisco or IEEE. If the device does not draw power, the value is n/a. The display shows Cisco when the device is a Cisco powered device. IEEE indicates that the device is an IEEE 802.3af- compliant powered device.

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show priority-queue statistics

To display the priority-queue statistics for an interface, use the **show priority-queue statistics** command in privileged EXEC mode.

show priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command shows priority-queue statistics for all configured interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the **show priority-queue statistics** command for the interface named test, and the command output. In this output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
clear priority-queue statistics	Clears the priority-queue statistics counters for an interface or for all configured interfaces
priority-queue	Configures priority queueing on an interface.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

show processes

To display a list of the processes that are running on the security appliance, use the **show processes** command in privileged EXEC mode.

show processes [cpu-usage | *non-zero* **|** *sorted***] [cpu-hog | memory | internals]**

Syntax Description

non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes

Defaults

By default this command displays the processes running on the security appliance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	Support for this command was introduced.
7.0(4)	The Runtime value was enhanced to display accurracy within one millisecond.
7.2(1)	The output display was enhanced to display more detailed information about processes that hog the CPU.
8.0(1)	Added the **show process cpu-usage** argument.

Usage Guidelines

The **show processes** command allows you to display a list of the processes that are running on the security appliance.

The command can also help determine what process is using the CPU, with the optional **cpu-usage or cpu-hog** arguments. A process is flagged if it is hogging the CPU for more than 100 milliseconds.

The **show process cpu-usage** command displays the processes running on the security appliance and the CPU usage statistics for the last 5 seconds, 1 minute and 5 minutes. The security appliance administrators can use this command to narrow down a particular process on the security appliance that might be utilizing the CPU of the security appliance. The additional arguments *sorted* and *non-zero* can be used to further customize the output of the command.

The **show process cpu-hog** command displays the following columns when invoked:

- MAXHOG - Maximum CPU hog runtime in milliseconds.
- NUMHOG - Number of CPU hog runs.
- LASTHOG - Last CPU hog runtime in milliseconds.
- PC - Instruction pointer of the CPU hogging process
- Traceback - Stack trace of the CPU hogging process

Processes are lightweight threads requiring only a few instructions. In the listing, PC is the program counter, SP is the stack pointer, STATE is the address of a thread queue, Runtime is the number of milliseconds that the thread has been running based on CPU clock cycles, SBASE is the stack base address, Stack is the current number of bytes that are used and the total size of the stack, and Process lists the thread's function.

The runtime value displays accurracy within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (<10ns resolution) instead of clock ticks (10ms resolution).

The traceback can have up to 14 addresses.

With the scheduler and total summary lines, you can run two consecutive **show proccess** commands and compare the output to determine:

- Where 100% of the CPU time was spent.
- What % of CPU is used by each thread, by comparing a thread's runtime delta to the total runtime delta.

The optional **memory** argument displays the memory allocated by each process, to help track memory usage by process.

The optional **internals** argument displays the number of invoked calls and giveups. Invoked is the number of times the scheduler has invoked, or ran, the process. Giveups is the number of times the process yielded the CPU back to the scheduler.

Examples

This example shows how to display a list of processes that are running on the security appliance:

```
hostname(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total

hostname(config)# show proc cpu-usage non-zero
PC         Thread     5Sec    1Min    5Min    Process
0818af8e   d482f92c   0.1%    0.1%    0.1%    Dispatch Unit
08bae136   d48180f0   0.1%    0.0%    0.2%    ssh
-------------------------------------

hostname(config)# show processes cpu

Process: ci/console, NUMHOG: 1, MAXHOG: 210, LASTHOG: 210 LASTHOG At:  01:08:24 UTC Jul 24
2005
```

```
PC:          153412
Traceback:    1532de  15352a  14b66d  14ba61 148c30 14930e  1125d1

Process: fover_parse, NUMHOG: 2, MAXHOG: 200, LASTHOG: 200
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           6ff434
Traceback:    6ff838  6fe3a7  6fe424  6fe5ab 7060b7 3bfa44  1125d1

hostname(config)# show processes memory

------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)


hostname# show processes internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

show reload

To display the reload status on the security appliance, use the **show reload** command in privileged EXEC mode.

show reload

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows that a reload is scheduled for 12:00 a.m. (midnight) on Saturday, April 20:

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

Related Commands

Command	Description
reload	Reboots and reloads the configuration.

show resource allocation

To show the resource allocation for each resource across all classes and class members, use the **show resource allocation** command in privileged EXEC mode.

show resource allocation [**detail**]

Syntax Description

detail	Shows additional information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command shows the resource allocation, but does not show the actual resources being used. See the **show resource usage** command for more information about actual resource usage.

Examples

The following is sample output from the **show resource allocation** command. The display shows the total allocation of each resource as an absolute value and as a percentage of the available system resources.

```
hostname# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Xlates                     91749           N/A
 All                    unlimited
```

Table 27-10 shows each field description.

Table 27-10 show resource allocation Fields

Field	Description
Resource	The name of the resource that you can limit.
Total	The total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the security appliance converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts, if available. If a resource does not have a system limit, this column shows N/A.

The following is sample output from the **show resource allocation detail** command:

```
hostname# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
```

```
                  All Contexts:      3                              20      20.00%

Xlates            default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      23040      23040      N/A
                  bronze             0      CA      11520
                  All Contexts:      3                         23040      N/A

mac-addresses     default          all       C      65535
                  gold               1       D      65535      65535    100.00%
                  silver             1      CA       6553       6553      9.99%
                  bronze             0      CA       3276
                  All Contexts:      3                         137623    209.99%
```

Table 27-11 shows each field description.

Table 27-11 show resource allocation detail Fields

Field	Description
Resource	The name of the resource that you can limit.
Class	The name of each class, including the default class. The All contexts field shows the total values across all classes.
Mmbrs	The number of contexts assigned to each class.
Origin	The origin of the resource limit, as follows: • A—You set this limit with the **all** option, instead of as an individual resource. • C—This limit is derived from the member class. • D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be “C” instead of “D.” The security appliance can combine “A” with “C” or “D.”
Limit	The limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the security appliance converts the percentage to an absolute number for this display.
Total	The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	The percentage of the total system resources that is allocated across all contexts in the class, if available. If the resource is unlimited, this display is blank. If the resource does not have a system limit, this column shows N/A.

Related Commands

Command	Description
class	Creates a resource class.
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows the resource types for which you can set limits.
show resource usage	Shows the resource usage of the security appliance.

show resource types

To view the resource types for which the security appliance tracks usage, use the **show resource types** command in privileged EXEC mode.

show resource types

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command shows additional resource types that you can manage for each context.

Examples

The following sample display shows the resource types:

```
hostname# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

Related Commands

Command	Description
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
show resource usage	Shows the resource usage of the security appliance.

show resource usage

To view the resource usage of the security appliance or for each context in multiple mode, use the **show resource usage** command in privileged EXEC mode.

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to view statistics. Specify **all** for all contexts; the security appliance lists the context usage for each context.
count_threshold	Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count_threshold* applies to the current usage. **Note** To show all resources, set the *count_threshold* to **0**.
counter *counter_name*	Shows counts for the following counter types: • **current**—Shows the active concurrent instances or the current rate of the resource. • **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted. • **denied**—Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column. • **all**—(Default) Shows all statistics.
detail	Shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.

resource [**rate**] *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to show the rate of usage of a resource. Resources that are measured by rate include **conns**, **inspects**, and **syslogs**. You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm**—ASDM management sessions. • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects**—Application inspections. • **hosts**—Hosts that can connect through the security appliance. • **mac-addresses**—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **ssh**—SSH sessions. • **syslogs**—System log messages. • **telnet**—Telnet sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Shows all context usage combined.
system	(Multiple mode only) Shows all context usage combined, but shows the system limits for resources instead of the combined context limits.
top *n*	(Multiple mode only) Shows the contexts that are the top *n* users of the specified resource. You must specify a single resource type, and not **resource all**, with this option.

Defaults

For multiple context mode, the default context is **all**, which shows resource usage for every context. For single mode, the context name is ignored and the output shows the "context" as "System."

The default resource name is **all**, which shows all resource types.

The default counter name is **all**, which shows all statistics.

The default count threshold is **1**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command now shows the denied resources, because you can now limit the resources for each context.

Examples

The following is sample output from the **show resource usage context** command, which shows the resource usage for the admin context:

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

The following is sample output from the **show resource usage summary** command, which shows the resource usage for all contexts and all resources. This sample shows the limits for 6 contexts.

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

The following is sample output from the **show resource usage system** command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits:

```
hostname# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

The following is sample output from the **show resource usage detail counter all 0** command, which shows all resources, and not just those you can manage:

```
hostname# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
```

```
chunk:ether                 0           0  unlimited            0 admin
chunk:est                   0           0  unlimited            0 admin

...

Telnet                      0           0          5            0 admin
SSH                         1           1          5            0 admin
ASDM                        0           1          5            0 admin
Syslogs [rate]              0          68  unlimited            0 admin
aaa rate                    0           0  unlimited            0 admin
url filter rate             0           0  unlimited            0 admin
Conns                       1           6  unlimited            0 admin
Xlates                      0           0  unlimited            0 admin
tcp conns                   0           0  unlimited            0 admin
Hosts                       2           3  unlimited            0 admin
udp conns                   0           0  unlimited            0 admin
smtp-fixups                 0           0  unlimited            0 admin
Conns [rate]                0           7  unlimited            0 admin
establisheds                0           0  unlimited            0 admin
pps                         0           0  unlimited            0 admin
syslog rate                 0           0  unlimited            0 admin
bps                         0           0  unlimited            0 admin
Fixups [rate]               0           0  unlimited            0 admin
non tcp/udp conns           0           0  unlimited            0 admin
tcp-intercepts              0           0  unlimited            0 admin
globals                     0           0  unlimited            0 admin
np-statics                  0           0  unlimited            0 admin
statics                     0           0  unlimited            0 admin
nats                        0           0  unlimited            0 admin
ace-rules                   0           0        N/A            0 admin
aaa-user-aces               0           0        N/A            0 admin
filter-rules                0           0        N/A            0 admin
est-rules                   0           0        N/A            0 admin
aaa-rules                   0           0        N/A            0 admin
console-access-rul          0           0        N/A            0 admin
policy-nat-rules            0           0        N/A            0 admin
fixup-rules                 0           0        N/A            0 admin
aaa-uxlates                 0           0  unlimited            0 admin
CP-Traffic:IP               0           0  unlimited            0 admin
CP-Traffic:ARP              0           0  unlimited            0 admin
CP-Traffic:Fixup            0           0  unlimited            0 admin
CP-Traffic:NPCP             0           0  unlimited            0 admin
CP-Traffic:Unknown          0           0  unlimited            0 admin
```

Related Commands

Command	Description
class	Creates a resource class.
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows a list of resource types.

show rip database

To display the information contained in the RIP topological database, use the **show rip database** command in privileged EXEC mode.

show rip database [*ip_addr* [*mask*]]

Syntax Description

ip_addr	(Optional) Limits the display routes for the specified network address.
mask	(Optional) Specifies the network mask for the optional network address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The RIP routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an RIP configuration mode to use the RIP-related **show** commands.

The RIP database contains all of the routes learned through RIP. Routes that appear in this database may not necessarily appear in the routing table. Refer to the *Cisco Security Appliance Command Line Configuration Guide* for information about how the routing table is populated from the routing protocol databases.

Examples

The following is sample output from the **show rip database** command:

```
hostname# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

The following is sample output from the **show rip database** command with a network address and mask:

```
Router# show rip database 172.19.86.0 255.255.255.0
```

```
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

Related Commands

Command	Description
router rip	Enables RIP routing and configures global RIP routing parameters.

show route

To display the routing table, use the **show route** command in privileged EXEC mode.

show route [*interface_name* [*ip_address* [*netmask* [**static**]]]]

Syntax Description

static	(Optional) Limits the display to static routes.
interface_name	(Optional) Limits the display to route entries that use the specified interface.
ip_address	(Optional) Limits the display to routes to the specified destination.
netmask	(Optional) Network mask to apply to *ip_address*.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show route** command:

```
hostname# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

The following is sample output of the show route command on the ASA5505 adaptive security appliance. It displays the internal loopback address, which is used by the VPN Hardware Client for individual user authentication.

```
hostname(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Creates a static or default route.
show running-config route	Displays the route commands in the running configuration.

CHAPTER 28

show running-config through show running-config isakmp Commands

show running-config

To display the configuration that is currently running on the security appliance, use the **show running-config** command in privileged EXEC mode.

show running-config [**all**] [*command*]

Syntax Description

all	Displays the entire operating configuration, including defaults.
command	Displays the configuration associated with a specific command.

Defaults

If no arguments or keywords are specified, the entire non-default security appliance configuration displays.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Pre-existing	This command was modified.

Usage Guidelines

The **show running-config** command displays the active configuration in memory (including saved configuration changes) on the security appliance.

You can use the **running-config** keyword only in the **show running-config** command. You cannot use this keyword with **no** or **clear**, or as a standalone command, because the CLI treats it as a nonsupported command. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

To display the saved configuration in flash memory on the security appliance, use the **show configuration** command.

Note ASDM commands appear in the configuration after you use it to connect to or configure the security appliance.

Examples

This example show how to display the active configuration that is running on the security appliance:

```
hostname# show running-config
: Saved
:
XXX Version X.X(X)
names
```

```
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
```

```
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

Related Commands

Command	Description
configure	Configures the security appliance from the terminal.

show running-config aaa

To show the AAA configuration in the running configuration, use the **show running-config aaa** command in privileged EXEC mode.

show running-config aaa [**accounting** | **authentication** | **authorization** | **mac-exempt** | **proxy-limit**]

Syntax Description

accounting	(Optional) Show accounting-related AAA configuration.
authentication	(Optional) Show authentication-related AAA configuration.
authorization	(Optional) Show authorization-related AAA configuration.
mac-exempt	(Optional) Show MAC address exemption AAA configuration.
proxy-limit	(Optional) Show the number of concurrent proxy connections allowed per user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config aaa** command:

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
hostname#
```

Related Commands

Command	Description
aaa authentication match	Enables authentication for traffic that is identified by an access list.
aaa authorization match	Enables authorization for traffic that is identified by an access list.

Command	Description
aaa accounting match	Enables accounting for traffic that is identified by an access list.
aaa max-exempt	Specifies the use of a predefined list of MAC addresses to exempt from authentication and authorization.
aaa proxy-limit	Configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user.

show running-config aaa-server

To display AAA server configuration, use the **show running-config aaa-server** command in privileged EXEC mode.

show running-config [**all**] **aaa-server** [*server-tag*] [**(***interface-name***)**] [**host** *hostname*]

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
host *hostname*	(Optional) The symbolic name or IP address of the particular host for which you want to display AAA server statistics.
(interface-name)	(Optional) The network interface where the AAA server resides.
server-tag	(Optional) The symbolic name of the server group.

Defaults

Omitting the *server-tag* value displays the configurations for all AAA servers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines

Usage Guidelines

Use this command to display the settings for a particular server group. Use the **all** parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the default AAA server group, use the following command:

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
hostname(config)#
```

Related Commands

Command	Description
show aaa-server	Displays AAA server statistics.
clear configure aaa-server	Clears the AAA server configuration.

show running-config aaa-server host

To display AAA server statistics for a particular server, use the **show running-config aaa-server** command in global configuration or privileged EXEC mode.

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
server-tag	The symbolic name of the server group.

Defaults

Omitting the default keyword displays only the explicitly configured configuration values, not the default values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to adhere to CLI guidelines.

Usage Guidelines

Use this command to display the statistics for a particular server group. Use the default parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the server group svrgrp1, use the following command:

```
hostname(config)# show running-config default aaa-server svrgrp1
```

Related Commands

Command	Description
show running-config aaa-server	Displays AAA server settings for the indicated server, group, or protocol.
clear configure aaa	Removes the settings for all AAA servers across all groups.

show running-config access-group

To display the access group information, use the **show running-config access-group** command in privileged EXEC mode.

show running-config access-group

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show running-config access-group** command:

```
hostname# show running-config access-group
access-group 100 in interface outside
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
clear configure access-group	Removes access groups from all the interfaces.

show running-config access-list

To display the access-list configuration that is running on the security appliance, use the **show running-config access-list** command in privileged EXEC mode.

show running-config [**default**] **access-list** [**alert-interval** | **deny-flow-max**]

show running-config [**default**] **access-list** *id* [*saddr_ip*]

Syntax Description

alert-interval	Shows the alert interval for generating syslog message 106001, which alerts that the system has reached a deny flow maximum.
deny-flow-max	Shows the maximum number of concurrent deny flows that can be created.
id	Identifies the access list that is displayed.
saddr_ip	Shows the access list elements that contain the specified source IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Usage Guidelines

The **show running-config access-list** command allows you to display the current running access list configuration on the security appliance.

Examples

The following is sample output from the **show running-config access-list** command:

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.

show running-config alias

To display the overlapping addresses with dual NAT commands in the configuration, use the **show running-config alias** command in privileged EXEC mode.

show running-config alias {*interface_name***}**

Syntax Description

interface_name	Internal network interface name that the destination_ip overwrites.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to display alias information:

```
hostname# show running-config alias
```

Related Commands

Command	Description
alias	Creates an alias.
clear configure alias	Deletes an alias.

show running-config arp

To show static ARP entries created by the **arp** command in the running configuration, use the **show running-config arp** command in privileged EXEC mode.

show running-config arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config arp** command:

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show running-config arp timeout

To view the ARP timeout configuration in the running configuration, use the **show running-config arp timeout** command in privileged EXEC mode.

show running-config arp timeout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show arp timeout**.

Examples

The following is sample output from the **show running-config arp timeout** command:

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp timeout	Sets the time before the security appliance rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.

show running-config arp-inspection

To view the ARP inspection configuration in the running configuration, use the **show running-config arp-inspection** command in privileged EXEC mode.

show running-config arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show arp timeout**.

Examples

The following is sample output from the **show running-config arp-inspection** command:

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.

show running-config asdm

To display the **asdm** commands in the running configuration, use the **show running-config asdm** command in privileged EXEC mode.

show running-config asdm [**group** | **location**]

Syntax Description

group	(Optional) Limits the display to the **asdm group** commands in the running configuration.
location	(Optional) Limits the display to the **asdm location** commands in the running configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **show running-config pdm** command to the **show running-config asdm** command.

Usage Guidelines

To remove the **asdm** commands from the configuration, use the **clear configure asdm** command.

Note On security appliances running in multiple context mode, the **show running-config asdm group** and **show running-config asdm location** commands are only available in the system execution space.

Examples

The following is sample output from the **show running-configuration asdm** command:

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.

show running-config auth-prompt

To displays the current authentication prompt challenge text, use the show running-config auth-prompt command in global configuration mode.

show running-config [default] auth-prompt

Syntax Description

default	(Optional) Display the default authentication prompt challenge text.

Defaults

Display the configured authentication prompt challenge text.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified for this release to conform to CLI guidelines.

Usage Guidelines

After you configure the authentication prompt with the **auth-prompt** command, use the **show running-config auth-prompt** command to view the current prompt text.

Examples

The following example shows the output of the **show running-config auth-prompt** command:

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
hostname(config)#
```

Related Commands

auth-prompt	Set the user authorization prompts.
clear configure auth-prompt	Reset the user authorization prompts to the default value.

show running-config banner

To display the specified banner and all the lines that are configured for it, use the **show running-config banner** command in privileged EXEC mode.

show running-config banner [**exec | login | motd**]

Syntax Description

exec	(Optional) Displays the banner before the enable prompt.
login	(Optional) Displays the banner before the password login prompt when accessing the security appliance using Telnet.
motd	(Optional) Displays the message-of-the-day banner.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The **running-config** keyword was added.

Usage Guidelines

The **show running-config banner** command displays the specified banner keyword and all the lines configured for it. If a keyword is not specified, then all banners display.

Examples

This example shows how to display the message-of-the-day (motd) banner:

```
hostname# show running-config banner motd
```

Related Commands

Command	Description
banner	Creates a banner.
clear configure banner	Deletes a banner.

show running-config class

To show the resource class configuration, use the **show running-config class** command in privileged EXEC mode.

show running-config class

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show running-config class** command:

```
hostname# show running-config class

class default
  limit-resource All 0
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
```

Related Commands

Command	Description
class	Configures a resource class.
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.

show running-config class-map

To display the information about the class map configuration, use the **show running-config class-map** command in privileged EXEC mode.

show running-config [**all**] **class-map** [*class_map_name* | **type** {**management** | **regex** | **inspect** [*protocol*]}]

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
class_map_name	(Optional) Shows the running configuration for a class map name.
inspect	(Optional) Shows inspection class maps.
management	(Optional) Shows management class maps.
protocol	(Optional) Specifies the type of application map you want to show. Available types include: • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	(Optional) Shows regular expression class maps.
type	(Optional) Specifies the type of class map you want to show. To show Layer 3/4 class maps, to not specify the type.

Defaults

The **class-map class-default** command, which contains a single **match any** command is the default class map.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config class-map** command:

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
hostname#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.

show running-config client-update

To display global client-update configuration information, use the **show running-config client-update** command in global configuration mode or in tunnel-group ipsec-attributes configuration mode.

show running-config client-update

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added tunnel-group ipsec-attributes configuration mode.

Usage Guidelines

Use this command to display global client-update configuration information.

Examples

This example shows a **show running-config client-update** command in global configuration mode and its output for a configuration with client-update enabled:

```
hostname(config)# show running-config client-update
hostname(config)# client-update enable
```

Related Commands

Command	Description
clear configure client-update	Clears the entire client-update configuration.
client-update	Configures client-update.

show running-config clock

To show the clock configuration in the running configuration, use the **show running-config clock** command in privileged EXEC mode.

show running-config [**all**] **clock**

Syntax Description

all	(Optional) Shows all **clock** commands, including the commands you have not changed from the default.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **all** keyword also displays the exact day and time for the **clock summer-time** command, as well as the default setting for the offset, if you did not originally set it.

Examples

The following is sample output from the **show running-config clock** command. Only the **clock summer-time** command was set.

```
hostname# show running-config clock
clock summer-time EDT recurring
```

The following is sample output from the **show running-config all clock** command. The default setting for the unconfigured **clock timezone** command displays, and the detailed information for the **clock summer-time** command displays.

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.

show running-config command-alias

To display the command aliases that are configured, use the **show running-config command-alias** command in privileged EXEC mode.

show running-config [**all**] **command-alias**

Syntax Description

all	(Optional) Displays all command aliases configured, including defaults.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you do not enter the **all** keyword, only non-default command aliases display.

Examples

The following example displays all command aliases that are configured on the security appliance, *including* defaults:

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

The following example displays all command aliases that are configured on the security appliance, *excluding* defaults:

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

Related Commands

Command	Description
command-alias	Creates a command alias.
clear configure command-alias	Deletes all non-default command aliases.

show running-config compression

To display the compression configuration in the running configuration, use the **show running-config compression** command from privileged EXEC mode:

show running-config compression

Defaults

There is no default behavior for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example shows the compression configuration within the running configuration:

```
hostname# show running-config compression
compression svc http-comp
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and Port Forwarding connections.

show running-config console timeout

To display the console connection timeout value, use the **show running-config console timeout** command in privileged EXEC mode.

show running-config console timeout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to display the console connection timeout setting:

```
hostname# show running-config console timeout
console timeout 0
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the security appliance.
clear configure console	Resets the console connection settings to defaults.

show running-config context

To show the context configuration in the system execution space, use the **show running-config context** command in privileged EXEC mode.

show running-config [**all**] **context**

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default. If you use the **mac-address auto** command, then you can view the assigned MAC addresses using the **all** keyword.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(5)	When using the **all** keyword, you can view assigned MAC addresses to shared interfaces when you configure the **mac-address auto** command.

Usage Guidelines

If you use the **mac-address auto** command to generate unique MAC addresses for shared interfaces, the **all** option is required to view the assigned MAC addresses. Although the **mac-address auto** command is user-configurable in global configuration mode only, the **mac-address auto** command appears as a read-only entry in the configuration for each context along with the assigned MAC address. Only shared interfaces that are configured with a **nameif** command within the context have a MAC address assigned.

Note If you manually assign a MAC address to an interface, but also have auto-generation enabled, the auto-generated address continues to show in the configuration even though the manual MAC address is the one that is in use. If you later remove the manual MAC address, the auto-generated one shown will be used.

Examples

The following output from the **show running-config all context admin** command shows the primary and standby MAC address assigned to the Management0/0 interface:

```
hostname# show running-config all context admin
```

```
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

The following output from the **show running-config all context** command shows all the MAC addresses (primary and standby) for all context interfaces. Note that because the GigabitEthernet0/0 and GigabitEthernet0/1 main interfaces are not configured with a **nameif** command inside the contexts, no MAC addresses have been generated for them.

```
hostname# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
mac-address auto	Automatically generates unique MAC addresses for shared interfaces.

show running-config crypto

To display the entire crypto configuration including IPSec, crypto maps, dynamic crypto maps, and ISAKMP, use the **show running-config crypto** command in global configuration or privileged EXEC mode.

show running-config crypto

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in privileged EXEC mode, displays all crypto configuration information:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto dynamic-map

To view a dynamic crypto map, use the **show running-config crypto dynamic-map** command in global configuration or privileged EXEC mode.

show running-config crypto dynamic-map

Syntax Description

This command has no keywords or arguments.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays all configuration information about crypto dynamic maps:

```
hostname(config)# show running-config crypto dynamic-map

Crypto Map Template "dyn1" 10

        access-list 152 permit ip host 172.21.114.67 any
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={ tauth, t1, }
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto ipsec

To display the complete IPSec configuration, use the **show running-config crypto ipsec** command in global configuration or privileged EXEC mode.

show running-config crypto ipsec

Syntax Description

This command has no default behavior or values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example issued in global configuration mode, displays information about the IPSec configuration:

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto isakmp

To display the complete ISAKMP configuration, use the **show running-config crypto isakmp** command in global configuration or privileged EXEC mode.

show running-config crypto isakmp

Syntax Description

This command has no default behavior or values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show running-config isakmp** command was introduced.
7.2(1)	This command was deprecated. The **show running-config crypto isakmp** command replaces it.

Examples

The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname(config)# show running-config crypto isakmp
crypto isakmp enable inside
crypto isakmp policy 1 authentication pre-share
crypto isakmp policy 1 encryption 3des
crypto isakmp policy 1 hash md5
crypto isakmp policy 1 group 2
crypto isakmp policy 1 lifetime 86400
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.

Command	Description
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show crypto isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto map

To display all configuration for all crypto maps, use the **show running-config crypto map** command in global configuration or privileged EXEC mode.

show running-config crypto map

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in privileged EXEC mode, displays all configuration information for all crypto maps:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config ctl-file

To show configured CTL file instances, use the **show running-config ctl-file** command in privileged EXEC mode.

show running-config [**all**] **ctl-file** [*ctl_name*]

Syntax Description

ctl_name	(Optional) Specifies the name of the CTL file instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **show running-config ctl-file** command to show configured CTL file instances:

```
hostname# show running-config all ctl-file asa_ctl
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

show running-config ctl-provider

To display all currently running Certificate Trust List provider configurations, use the **show running-config ctl-provider** command in privileged EXEC mode.

show running-config [**all**] **ctl-provider** [*provider_name*]

Syntax Description

all	Shows all TLS proxy commands, including the commands you have not changed from the default.
provider_name	Specifies the name of the CTL provider to show.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following is sample output of the **show running-config ctl-provider** command:

```
hostname# show running-config ctl-provider
ctl-provider ctl_prov
    client interface inside address 195.168.2.103
    client username CCMAdministrator password xxxxxxxxxxxx encrypted
    export certificate local_ccm
```

Related Commands

Command	Description
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.

show running-config ddns

To display the DDNS update methods of the running configuration, use the **show running-config ddns** command in privileged EXEC mode.

show running-config [**all**] **ddns** [**update**]

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
update	(Optional) Specifies that DDNS update method information be displayed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays the DDNS methods in the running configuration with test in the name:

```
hostname# show running-config all ddns | grep test
ddns update method test
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a security appliance interface with a DDNS update method or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
show ddns update interface	Displays the interfaces associated with each configured DDNS method.
show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.

show running-config dhcp-client

To display the DHCP client update parameters in the running configuration, use the **show running-config dhcp-client** command in privileged EXEC mode.

show running-config [**all**] **dhcp-client**

Syntax Description

all	(Optional) Shows the running configuration including default configuration values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays DHCP client update parameters in the running configuration that specify updates for both A and PTR records:

```
hostname# show running-config all dhcp-client | grep both
dhcp-client update dns server both
```

Related Commands

Command	Description
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
clear configure dhcp-client	Clears the DHCP client configuration.

show running-config dhcpd

To show the DHCP configuration, use the **show running-config dhcpd** command in privileged EXEC or global configuration mode.

show running-config dhcpd

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show dhcpd** command to the **show running-config dhcpd** command.

Usage Guidelines

The **show running-config dhcpd** command displays the DHCP commands entered in the running configuration. To see DHCP binding, state, and statistical information, use the **show dhcpd** command.

Examples

The following is sample output from the **show running-config dhcpd** command:

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
debug dhcpd	Displays debug information for the DHCP server.
show dhcpd	Displays DHCP binding, statistic, or state information.

show running-config dhcprelay

To view the current DHCP relay agent configuration, use the **show running-config dhcprelay** command in privileged EXEC mode.

show running-config dhcprelay

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config dhcprelay** command displays the current DHCP relay agent configuration. To show DHCP relay agent packet statistics, use the **show dhcprelay statistics** command.

Examples

The following example shows output from the **show running-config dhcprelay** command:

```
hostname(config)# show running-config dhcprelay

dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.

show running-config dns

To show the DNS configuration in the running configuration, use the **show running-config dns** command in privileged EXEC mode.

show running-config dns

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-config dns** command:

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

show running-config dns server-group

To show the DNS configuration in the running configuration, use the **show running-config dns** command in privileged EXEC mode.

show [**all**] **running-config dns server-group** [*name*]

Syntax Description

all	Displays the default and explicitly configured configuration information for one or all dns-server-groups.
name	Specifies the name of the dns server group for which you want to show the configuration information.

Defaults

If you omit the dns-server-group name, this command displays all the existing dns-server-group configurations.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.1 (1)	This command was introduced.

Examples

The following is sample output from the **show running-config dns server-group** command:

```
hostname# show running-config dns server-group
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 90.1.1.22
 domain-name frqa.cisco.com
dns server-group writers1
 retries 10
 timeout 3
 name-server 10.86.194.61
 domain-name doc-group
hostname#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters DNS server group mode, in which you can configure a DNS server group.

show running-config domain-name

To show the domain name configuration in the running configuration, use the **show running-config domain-name** command in privileged EXEC mode.

show running-config domain-name

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from **show domain-name**.

Examples

The following is sample output from the **show running-config domain-name** command:

```
hostname# show running-config domain-name
example.com
```

Related Commands

Command	Description
domain-name	Sets the default domain name.
hostname	Sets the security appliance hostname.

show running-config dynamic-access-policy-record

To display the running configuration for all DAP records, or for the named DAP record, use the **show running-config dynamic-access-policy-record** command in privileged EXEC mode.

show running-config dynamic-access-policy-record [*name***]**

Syntax DescriptionE

name	Specifies the name of the DAP record. The name can be up to 64 characters long and cannot contain spaces.

Defaults

All attributes display.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

This example shows the use of the **show running-config dynamic-access-policy-record** command to display statistics for the DAP record named Finance:

```
ASA(config)#show running-config dynamic-access-policy-record Finance
dynamic-access-policy-record Finance
description value "Finance users from trusted device"
network-acl FinanceFirewallAcl
user-message "Limit access to the Finance network"
priority 2
webvpn
  appl-acl FinanceWebvpnAcl
  url-list value FinanceLinks,StockLinks
  port-forward enable FinanceApps
  file-browsing enable
  file-entry enablehostname#
```

Related Commands

Command	Description
clear config dynamic-access-policy-record [*name***]**	Removes all DAP records or the named DAP record.
dynamic-access-policy-record	Creates a DAP record.

show running-config enable

To show the encrypted enable passwords, use the **show running-config enable** command in privileged EXEC mode.

show running-config enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **show enable** command.

Usage Guidelines

The password is saved to the configuration in encrypted form, so you cannot view the original password after you enter it. The password displays with the **encrypted** keyword to indicate that the password is encrypted.

Examples

The following is sample output from the **show running-config enable** command:

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.

show running-config established

To display the allowed inbound connections that are based on established connections, use the **show running-config established** command in privileged EXEC mode.

show running-config established

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **running-config** was added.

Usage Guidelines

This command has no usage guidelines.

Examples

This example shows how to display inbound connections that are based on established connections:

```
hostname# show running-config established
```

Related Commands

Command	Description
established	Permits return connections on ports that are based on an established connection.
clear configure established	Removes all established commands.

show running-config failover

To display the **failover** commands in the configuration, use the **show running-config failover** command in privileged EXEC mode.

show running-config [**all**] **failover**

Syntax Description

all	(Optional) Shows all failover commands, including the commands you have not changed from the default.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config failover** command displays the **failover** commands in the running configuration. It does not display the **monitor-interface** or **join-failover-group** commands.

Examples

The following example shows the default failover configuration before failover has been configured:

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
```

Related Commands

Command	Description
show failover	Displays failover state and statistics.

show running-config filter

To show the filtering configuration, use the **show running-config filter** command in privileged EXEC mode.

show running-config filter

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config filter** command displays the filtering configuration for the security appliance.

Examples

The following is sample output from the **show running-config filter** command, and shows the filtering configuration for the security appliance:

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

This example shows ActiveX filtering is enabled on port80 for the address 10.86.194.170.

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.

show running-config fips

To display the FIPS configuration that is running on the security appliance, use the **show running-config fips** command.

show running-config fips

Syntax Description

fips	FIPS-2 compliance information

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **show running-config fips** command allows you to display the current running fips configuration. You use the **running-config** keyword only in the **show running-config fips** command. You cannot use this keyword with no or clear, or as a standalone command as it is not supported. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

Examples

```
hostname(config)# show running-config fips
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.

show running-config fragment

To display the current configuration of the fragment databases, use the **show running-config fragment** command in privileged EXEC mode.

show running-config fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an interface is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config fragment** command displays the current configuration of the fragment databases. If you specify an interface name, only information for the database residing at the specified interface displays. If you do not specify an interface name, the command applies to all interfaces.

Use the **show running-config fragment** command to display this information:

- Size—Maximum number of packets set by the **size** keyword. This value is the maximum number of fragments that are allowed on the interface.
- Chain—Maximum number of fragments for a single packet set by the **chain** keyword.
- Timeout—Maximum number of seconds set by the **timeout** keyword. This is the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Examples

The following example shows how to display the states of the fragment databases on all interfaces:

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

```
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on interfaces that start with the name “outside”:

Note In this example, the interfaces named “outside1”, “outside2”, and “outside3” display.

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on the interfaces named “outside1” only:

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show fragment	Displays the operational data of the IP fragment reassembly module.

show running-config ftp mode

To show the client mode configured for FTP, use the **show running-config ftp mode** command in privileged EXEC mode.

show running-config ftp mode

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config ftp mode** command displays the client mode that is used by the security appliance when accessing an FTP server.

Examples

The following is sample output from the **show running-config ftp-mode** command:

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

Related Commands

Commands	Description
copy	Uploads or downloads image files or configuration files to or from an FTP server.
debug ftp client	Displays detailed information about FTP client activity.
ftp mode passive	Sets the FTP client mode used by the security appliance when accessing an FTP server.

show running-config global

To display the **global** commands in the configuration, use the **show running-config global** command in privileged EXEC mode.

show running-config global

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config global** command:

```
hostname# show running-config global
global (outside1) 10 interface
```

Related Commands

Command	Description
clear configure global	Removes **global** commands from the configuration.
global	Creates entries from a pool of global addresses.

show running-config group-delimiter

To display the current delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **show running-config group-delimiter** command in global configuration mode or in tunnel-group ipsec-attributes configuration mode.

show running-config group-delimiter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added tunnel-group ipsec-attributes configuration mode.

Usage Guidelines

Use this command to display the currently configured group-delimiter.

Examples

This example shows a **show running-config group-delimiter** command and its output:

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

Related Commands

Command	Description
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.

show running-config group-policy

To display the running configuration for a particular group policy, use the **show running-config group-policy** command in privileged EXEC mode and append the name of the group policy. To display the running configuration for all group policies, use this command without naming a specific group policy. To have either display include the default configuration, use the **all** keyword.

show running-config [all] group-policy [*name***]**

Syntax Description

all	(Optional) Displays the running configuration including default values.
name	(Optional) Specifies the name of the group policy.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to display the running configuration, including default values, for the group policy named FirstGroup:

```
hostname# show running-config all group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Creates, edits, or removes a group policy.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy.
clear config group-policy	Removes the configuration for a particular group policy or for all group policies.

show running-config http

To display the current set of configured http commands, use the **show running-config http** command in privileged EXEC mode.

show running-config http

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following sample output shows how to use the **show running-config http** command:

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

Related Commands

Command	Description
clear http	Remove the HTTP configuration: disable the HTTP server and remove hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.

show running-config icmp

To show the access rules configured for ICMP traffic, use the **show running-config icmp** command in privileged EXEC mode.

show running-config icmp *map_name*

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config icmp** command displays the access rules configured for ICMP traffic.

Examples

The following is sample output from the **show running-config icmp** command:

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

show running-config imap4s

To display the running configuration for IMAP4S, use the s**how running-config imap4s** command in privileged EXEC mode.

show running-config [all] imap4s

Syntax Description

all	(Optional) Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was introduced.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn	•	—	•	—	—

Examples

The following is sample output from the **show running-config imap4s** command:

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
imap4s	Creates or edits an IMAP4S e-mail proxy configuration.

show running-config interface

To show the interface configuration in the running configuration, use the s**how running-config interface** command in privileged EXEC mode.

show running-config [**all**] **interface** [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

all	(Optional) Shows all **interface** commands, including the commands you have not changed from the default.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the configuration for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following is sample output from the **show running-config interface** command. The following example shows the running configuration for all interfaces. The GigabitEthernet0/2 and 0/3 interfaces have not been configured yet, and show the default configuration. The Management0/0 interface also shows the default settings.

```
hostname# show running-config interface
!
interface GigabitEthernet0/0
```

```
 no shutdown
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 no shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/1.1
 vlan 101
 no shutdown
 nameif dmz
 security-level 50
 ip address 10.50.1.1 255.255.255.0
 mac-address 000C.F142.4CDE standby 020C.F142.4CDE
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 security-level 0
 no ip address
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show running-config ip address

To show the IP address configuration in the running configuration, use the s**how running-config ip address** command in privileged EXEC mode.

show running-config ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the IP address configuration for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

In transparent firewall mode, do not specify an interface because this command shows only the management IP address; the transparent firewall does not have IP addresses associated with interfaces.

This display also shows the **nameif** command and **security-level** command configuration.

Examples

The following is sample output from the **show running-config ip address** command:

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
```

```
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
security-level	Sets the security level for the interface.

show running-config ip audit attack

To show the **ip audit attack** configuration in the running configuration, use the **show running-config ip audit attack** command in privileged EXEC mode.

show running-config ip audit attack

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip audit attack**.

Examples

The following is sample output from the **show running-config ip audit attack** command:

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit info

To show the **ip audit info** configuration in the running configuration, use the **show running-config ip audit info** command in privileged EXEC mode.

show running-config ip audit info

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip audit info**.

Examples

The following is sample output from the **show running-config ip audit info** command:

```
hostname# show running-config ip audit info
ip audit info action drop
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit interface

To show the **ip audit interface** configuration in the running configuration, use the **show running-config ip audit interface** command in privileged EXEC mode.

show running-config ip audit interface [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the interface name.

Defaults

If you do not specify an interface name, this command shows the configuration for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip audit interface**.

Examples

The following is sample output from the **show running-config ip audit interface** command:

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit name

To show the **ip audit name** configuration in the running configuration, use the **show running-config ip audit name** command in privileged EXEC mode.

show running-config ip audit name [*name* [**info** | **attack**]]

Syntax Description

attack	(Optional) Shows the named audit policy configuration for attack signatures.
info	(Optional) Shows the named audit policy configuration for informational signatures.
name	(Optional) Shows the configuration for the audit policy name created using the **ip audit name** command.

Defaults

If you do not specify a name, this command shows the configuration for all audit policies.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip audit name**.

Examples

The following is sample output from the **show running-config ip audit name** command:

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit signature

To show the **ip audit signature** configuration in the running configuration, use the **show running-config ip audit signature** command in privileged EXEC mode.

show running-config ip audit signature [*signature_number*]

Syntax Description

signature_number	(Optional) Shows the configuration for the signature number, if present. See the **ip audit signature** command for a list of supported signatures.

Defaults

If you do not specify a number, this command shows the configuration for all signatures.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip audit signature**.

Examples

The following is sample output from the **show running-config ip audit signature** command:

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip local pool

To display IP address pools, use the **show running-config ip local pool** command in privileged EXEC mode.

show running-config ip local pool [*poolname*]

Syntax Description

poolname	(Optional) Specifies the name of the IP address pool.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ip local pool** command:

```
hostname(config)# show running-config ip local pool firstpool

Pool            Begin           End             Mask            Free    In use
firstpool               10.20.30.40     10.20.30.50     255.255.255.0      11
    0
Available Addresses:
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools
ip local pool	Configures an IP address pool.

show running-config ip verify reverse-path

To show the **ip verify reverse-path** configuration in the running configuration, use the **show running-config ip verify reverse-path** command in privileged EXEC mode.

show running-config ip verify reverse-path [interface *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows the configuration for the specified interface.

Defaults

This command shows the configuration for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show ip verify reverse-path**.

Examples

The following is sample output from the **show ip verify statistics** command:

```
hostname# show running-config ip verify reverse-path
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.

show running-config ipv6

To display the IPv6 commands in the running configuration, use the **show running-config ipv6** command in privileged EXEC mode.

show running-config [**all**] **ipv6**

Syntax Description

all	(Optional) Shows all **ipv6** commands, including the commands you have not changed from the default, in the running configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ipv6** command:

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

Related Commands

Command	Description
debug ipv6	Displays IPv6 debug messages.
show ipv6 access-list	Displays the IPv6 access list.
show ipv6 interface	Displays the status of the IPv6 interfaces.
show ipv6 route	Displays the contents of the IPv6 routing table.
show ipv6 traffic	Displays IPv6 traffic statistics.

show running-config isakmp

To display the complete ISAKMP configuration, use the **show running-config isakmp** command in global configuration or privileged EXEC mode.

show running-config isakmp

Syntax Description

This command has no default behavior or values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	The **show running-config isakmp** command was introduced.
7.2(1)	This command was deprecated. The **show running-config crypto isakmp** command replaces it.

Examples

The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

CHAPTER 29

show running-config ldap through show running-config wccp Commands

show running-config ldap

To display the LDAP attribute name and value mappings in running LDAP attribute maps, use the **show running-config ldap** command in privileged EXEC mode.

show running-config [**all**] **ldap attribute-map** *name*

Syntax Description

all	Displays all LDAP attribute maps.
name	Specifies an individual LDAP attribute map for display.

Defaults

By default, all attribute maps, mapped names, and mapped values display.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to display the LDAP attribute name and value mappings contained in attribute maps running on your security appliance. You can display all the attribute maps using the **all** option, or you can display a single attribute map by specifying the map name. If you enter neither the **all** option nor an LDAP attribute map name, all attribute maps, mapped names, and mapped values display.

Examples

The following example, entered in privileged EXEC mode, displays the attribute name and value mappings for a specific running attribute map, “myldapmap”:

```
hostname# show running-config ldap attribute-map myldapmap
map-name Hours cVPN3000-Access-Hours
map-value Hours workDay Daytime
```

The following command displays all attribute name and value mappings within all running attribute maps:

```
hostname# show running-config all ldap attribute-map
```

Related Commands

Command	Description
ldap attribute-map (global config mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
map-value	Maps a user-defined attribute value to a Cisco attribute.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

show running-config logging

To display all currently running logging configurations, use the **show runnig-config logging** command in privileged EXEC mode.

show running-config [all] logging [level | disabled]

Syntax Description

all	(Optional) Displays the logging configuration, including commands whose settings that you have not changed from the default.
disabled	(Optional) Displays only the disabled system log message configuration.
level	(Optional) Displays only the configuration for system log messages with a non-default severity level.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0 (1)	This command was changed from the **show logging** command.

Examples

The following is an example of the **show running-config logging disabled** command:

```
hostname# show running-config logging disabled

no logging message 720067
```

Related Commands

Command	Description
logging message	Configures logging.
show logging	Shows the log buffer and other logging settings.

show running-config mac-address

To show the **mac-address auto** configuration in the running configuration, use the s**how running-config mac-address** command in privileged EXEC mode.

show running-config mac-address

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show running-config mac-address** command:

```
hostname# show running-config mac-address
no mac-address auto
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address	Manually sets the MAC address (active and standby) for a physical interface or subinterface. In multiple context mode, you can set different MAC addresses in each context for the same interface.
mac-address auto	Auto-generates MAC addresses (active and standby) for shared interfaces in multiple context mode.
show interface	Shows the interface characteristics, including the MAC address.

show running-config mac-address-table

To view the **mac-address-table static** and **mac-address-table aging-time** configuration in the running configuration, use the **show running-config mac-address-table** command in privileged EXEC mode.

show running-config mac-address-table

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config mac-learn** command:

```
hostname# show running-config mac-address-table
mac-address-table aging-time 50
mac-address-table static inside1 0010.7cbe.6101
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

show running-config mac-learn

To view the **mac-learn** configuration in the running configuration, use the **show running-config mac-learn** command in privileged EXEC mode.

show running-config mac-learn

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config mac-learn** command:

```
hostname# show running-config mac-learn
mac-learn disable
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

show running-config mac-list

To display a list of MAC addresses previously specified in a **mac-list** command with the indicated MAC list number, use the **show running-config mac-list** command in privileged EXEC mode.

show running-config mac-list *id*

Syntax Description

id	A hexadecimal MAC address list number.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

The **show running-config aaa** command displays the **mac-list** command statements as part of the AAA configuration.

Examples

The following example shows how to display a MAC address list with the *id* equal to adc:

```
hostname(config)# show running-config mac-list adc
mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

Related Commands

Command	Description
mac-list	Add a list of MAC addresses using a first-match search.
clear configure mac-list	Remove the indicated **mac-list** command statements.
show running-config aaa	Display the running AAA configuration values.

show running-config management-access

To display the name of the internal interface configured for management access, use the **show running-config management-access** command in privileged EXEC mode.

show running-config management-access

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface and display the result:

```
hostname# management-access inside
hostname# show running-config management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the security appliance.
management-access	Configures an internal interface for management access.

show running-config monitor-interface

To display all **monitor-interface** commands in the running configuration, use the **show running-config monitor-interface** command in privileged EXEC mode.

show running-config [all] monitor-interface

Syntax Description

all	(Optional) Shows all **monitor-interface** commands, including the commands you have not changed from the default.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **monitor-interface** command is enabled on all physical interfaces by default. You need to use the **all** keyword with this command to view this default configuration.

Examples

The following is sample output from the **show running-config monitor-interface** command. The first time the command is entered without the **all** keyword, so only the interface that has monitoring enabled appears in the output. The second time the command is entered with the **all** keyword, so the default **monitor-interface** configuration is also show.

```
hostname# show running-config monitor-interface
no monitor-interface outside
hostname#
hostname# show running-config all monitor-interface
monitor-interface inside
no monitor-interface outside
hostname#
```

Related Commands

Command	Description
monitor-interface	Enables health monitoring of a designated interface for failover purposes.
clear configure monitor-interface	Removes the **no monitor-interface** commands in the running configuration and restores the default interface health monitoring stance.

show running-config mroute

To display the static multicast route table in the configuration use the **show running-config mroute** command in privileged EXEC mode.

show running-config mroute [*dst* [*src*]]

Syntax Description

dst	The Class D address of the multicast group.
src	The IP address of the multicast source.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config mroute** command:

```
hostname# show running-config mroute
```

Related Commands

Command	Description
mroute	Configures a static multicast route.

show running-config mtu

To display the current maximum transmission unit block size, use the **show running-config mtu** command in privileged EXEC mode.

show running-config mtu [*interface_name*]

Syntax Description

interface_name	(Optional) Internal or external network interface name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show running-config mtu** command:

```
hostname# show running-config mtu
mtu outside 1500
mtu inside 1500
mtu dmz 1500
hostname# show running-config mtu outside
mtu outside 1500
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
mtu	Specifies the maximum transmission unit for an interface.

show running-config multicast-routing

To display the **multicast-routing** command, if present, in the running configuration, use the **show running-config multicast-routing** command in privileged EXEC mode.

show running-config multicast-routing

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config multicast-routing** command displays the **multicast-routing** command in the running configuration. Enter the **clear configure multicast-routing** command to remove the **multicast-routing** command from the running configuration.

Examples

The following is sample output from the **show running-config multicast-routing** command:

```
hostname# show running-config multicast-routing

multicast-routing
```

Related Commands

Command	Description
clear configure multicast-routing	Removes the **multicast-routing** command from the running configuration.
multicast-routing	Enables multicast routing on the security appliance.

show running-config nac-policy

To show the configuration of each NAC policy on the security appliance, use the **show running-config nac-policy** command in privileged EXEC mode.

show running-config [all] nac-policy [*nac-policy-name***]**

Syntax Description

all	Displays the entire operating configuration of the NAC policy, including default settings.
nac-policy-name	Name of the NAC policy present in the configuration of the security appliance.

Defaults

By default, the CLI displays the name and configuration of each NAC policy if you do not specify the *nac-policy-name.*

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows the configuration of NAC policies named nacapp1 and nacapp2:

```
hostname# show running-config nac-policy
nac-policy framework nac-framework
 default-acl acl-1
 reval-period 36000
 sq-period 300
 exempt-list os "Windows XP" filter acl-2
nac-policy nacapp1 nacapp
 auth-vlan 1
 cas 209.165.202.129
 cam outside 209.165.201.22 community secretword
timeout 10
hostname#
```

The first line of each NAC policy indicates its name and type. The types are as follows:

- `nacapp` uses a Cisco NAC Appliance to provide a network access policy for remote hosts. Table 29-1 explains the nacapp attributes displayed in response to the **show running-config nac-policy** command.

- `nac-framework` uses a Cisco Access Control Server to provide a network access policy for remote hosts. Table 29-2 explains the nac-framework attributes displayed in response to the **show running-config nac-policy** command.

Table 29-1 show running-config nac-policy Command Fields for nacapp policies

Field	Description
`auth-vlan`	Authentication VLAN that provides the user with limited access while posture validation is in progress. Upon completion of the tunnel, the security appliance copies the value of the auth-vlan to the vlan attribute assigned to the session. Following a successful posture validation, the security appliance overwrites the value of the vlan attribute with the value of the access VLAN obtained from the NAC Appliance.
`cam`	This line shows the following values: • Interface on the security appliance through which to communicate with the Clean Access Manager. • IP address or hostname of the CAM. • SNMP community string on the CAM.
`cas`	IP address or hostname of the Clean Access Server.
`timeout`	Maximum number of minutes a user session can be assigned to an authentication VLAN.

Table 29-2 show running-config nac-policy Command Fields for nac-framework policies

Field	Description
`default-acl`	NAC default ACL applied before posture validation. Following posture validation, the security appliance replaces the default ACL with the one obtained from the Access Control Server for the remote host. It retains the default ACL if posture validation fails.
`reval-period`	Number of seconds between each successful posture validation in a NAC Framework session.
`sq-period`	Number of seconds between each successful posture validation in a NAC Framework session and the next query for changes in the host posture
`exempt-list`	Operating system names that are exempt from posture validation. Also shows an optional ACL to filter the traffic if the remote computer's operating system matches the name.
`authentication-server-group`	name of the of authentication server group to be used for NAC posture validation.

Related Commands

nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
clear configure nac-policy	Removes all NAC policies from the running configuration except for those that are assigned to group policies.
show nac-policy	Displays NAC policy usage statistics on the security appliance.
show vpn-session_summary.db	Displays the number IPSec, Cisco AnyConnect, and NAC sessions, including VLAN mapping session data.
show vpn-session.db	Displays information about VPN sessions, including VLAN mapping and NAC results.

show running-config name

To display a list of names associated with IP addresses (configured with the **name** command), use the **show running-config name** command in privileged EXEC mode.

show running-config name

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to display a list of names associated with IP addresses:

```
hostname# show running-config name
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.

show running-config nameif

To show the interface name configuration in the running configuration, use the s**how running-config nameif** command in privileged EXEC mode.

show running-config nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the interface name configuration for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from **show nameif**.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context.

This display also shows the **security-level** command configuration.

Examples

The following is sample output from the **show running-config nameif** command:

```
hostname# show running-config nameif
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
!
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
security-level	Sets the security level for the interface.

show running-config names

To display the IP address-to-name conversions, use the **show running-config names** command in privileged EXEC mode.

show running-config names

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use with the **names** command.

Examples

The following example shows how to display the IP address-to-name conversion:

```
hostname# show running-config names
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.
names	Enables IP address-to-name conversions that you can configured with the **name** command.
show running-config name	Displays a list of names associated with IP addresses.

show running-config nat

To display a pool of global IP addresses that are associated with a network, use the **show running-config nat** command in privileged EXEC mode.

show running-config nat [*interface_name*] [*nat_id*]

Syntax Description

interface_name	(Optional) Name of the network interface.
nat_id	(Optional) ID of the group of host or networks.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Usage Guidelines

This command displays the maximum connection value for the UDP protocol. Every time the UPD maximum connection value is not set, the value will be displayed as 0 by default and will not be applied.

Note In transparent mode, only NAT ID 0 is valid.

Examples

This example shows how to display a pool of global IP addresses that are associated with a network:

```
hostname# show running-config nat
nat (inside) 1001 10.7.2.0 255.255.255.224 0 0
nat (inside) 1001 10.7.2.32 255.255.255.224 0 0
nat (inside) 1001 10.7.2.64 255.255.255.224 0 0
nat (inside) 1002 10.7.2.96 255.255.255.224 0 0
nat (inside) 1002 10.7.2.128 255.255.255.224 0 0
nat (inside) 1002 10.7.2.160 255.255.255.224 0 0
nat (inside) 1003 10.7.2.192 255.255.255.224 0 0
nat (inside) 1003 10.7.2.224 255.255.255.224 0 0
```

Related Commands

Command	Description
clear configure nat	Removes the NAT configuration.
nat	Associates a network with a pool of global IP addresses.

show running-config nat-control

To show the NAT configuration requirement, use the **show running-config nat-control** command in privileged EXEC mode.

show running-config nat-control

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config nat-control** command:

```
hostname# show running-config nat-control
no nat-control
```

Related Commands

Command	Description
nat	Defines an address on one interface that is translated to a global address on another interface.
nat-control	Allows inside hosts to communicate with outside networks without configuring a NAT rule.

show running-config ntp

To show the NTP configuration in the running configuration, use the **show running-config ntp** command in privileged EXEC mode.

show running-config ntp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config ntp** command:

```
hostname# show running-config ntp
ntp authentication-key 1 md5 test2
ntp authentication-key 2 md5 test
ntp trusted-key 1
ntp trusted-key 2
ntp server 10.1.1.1 key 1
ntp server 10.2.1.1 key 2 prefer
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show running-config object-group

To display the current object groups, use the **show running-config object-group** command in privileged EXEC mode.

show running-config [**all**] **object-group** [**protocol** | **service** | **network** | **icmp-type** | **id** *obj_grp_id*]

Syntax Description

icmp-type	(Optional) Displays ICMP type object groups.
id obj_grp_id	(Optional) Displays the specified object group.
network	(Optional) Displays network object groups.
protocol	(Optional) Displays protocol object groups.
service	(Optional) Displays service object groups.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show running-config object-group** command:

```
hostname# show running-config object-group
object-group protocol proto_grp_1
    protocol-object udp
    protocol-object tcp
object-group service eng_service tcp
    port-object eq smtp
    port-object eq telnet
object-group icmp-type icmp-allowed
    icmp-object echo
    icmp-object time-exceeded
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.

show running-config passwd

To show the encrypted login passwords, use the **show running-config passwd** command in privileged EXEC mode.

show running-config {**passwd** | **password**}

Syntax Description

passwd | **password**	You can enter either command; they are aliased to each other.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **show passwd** command.

Usage Guidelines

The password is saved to the configuration in encrypted form, so you cannot view the original password after you enter it. The password displays with the **encrypted** keyword to indicate that the password is encrypted.

Examples

The following is sample output from the **show running-config passwd** command:

```
hostname# show running-config passwd
passwd 2AfK9Kjr3BE2/J2r encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
passwd	Sets the login password.
show curpriv	Shows the currently logged in username and the user privilege level.

show running-config phone-proxy

To show Phone Proxy specific information, use the **show running-config phone-proxy** command in privileged EXEC mode.

show running-config [**all**] **phone-proxy** [*phone_proxy_name*]

Syntax Description

phone_proxy_name	(Optional) Specifies the name of the Phone Proxy instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Examples

The following example shows the use of the **show running-config phone-proxy** command to show Phone Proxy specific information:

```
hostname# show running-config all phone proxy asa_phone_proxy
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

show running-config pim

To display the PIM commands in the running configuration, use the **show running-config pim** command in privileged EXEC mode.

show running-config pim

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config pim** command displays the **pim** commands entered in global configuration mode. It does not show the **pim** commands entered in interface configuration mode. To see the **pim** commands entered in interface configuration mode, enter the **show running-config interface** command.

Examples

The following is sample output from the **show running-config pim** command:

```
hostname# show running-config pim

pim old-register-checksum
pim spt-threshold infinity
```

Related Commands

Command	Description
clear configure pim	Removes the **pim** commands from the running configuration.
show running-config interface	Displays interface configuration commands entered in interface configuration mode.

show running-config policy-map

To display all the policy-map configurations or the default policy-map configuration, use the **show running-config policy-map** command in privileged EXEC mode.

show running-config [all] policy-map [*policy_map_name* | **type inspect** [*protocol*]]

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
policy_map_name	(Optional) Shows the running configuration for a policy map name.
protocol	(Optional) Specifies the type of inspection policy map you want to show. Available types include: • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**
type inspect	(Optional) Shows inspection policy maps.

Defaults

Omitting the **all** keyword displays only the explicitly configured policy-map configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Specifying the **all** keyword displays the default policy-map configuration as well as the explicitly configured policy-map configuration.

Examples

The following is sample output from the **show running-config policy-map** command:

```
hostname# show running-config policy-map
!
policy-map localmap1
    description this is a test.
    class firstclass
    priority
    ids promiscuous fail0close
    set connection random-seq# enable
    class class-default
!
```

Related Commands

Command	Description
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure policy-map	Removes the entire policy configuration.

show running-config pop3s

To display the running configuration for POP3S, use the s**how running-config pop3s** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] pop3s

Syntax Description

all	Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was introduced.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn	•	—	•	—	—

Examples

The following is sample output from the **show running-config pop3s** command:

```
hostname# show running-config pop3s

pop3s
 server 10.160.102.188
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all pop3s

pop3s
 port 995
 server 10.160.102.188
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.
pop3s	Creates or edits a POP3S e-mail proxy configuration.

show running-config prefix-list

To display the **prefix-list** command in the running configuration, use the **show running-config prefix-list** command in privileged EXEC mode.

show running-config prefix-list

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show prefix-list** command to the **show running-config prefix-list** command.

Usage Guidelines

The **prefix-list description** commands always appear before their associated **prefix-list** commands in the running configuration. It does not matter what order you entered them.

Examples

The following is sample output from the **show running-config prefix-list** command:

```
hostname# show running-config prefix-list

!
prefix-list abc description A sample prefix list
prefix-list abc seq 5 permit 192.168.0.0/8 le 24
prefix-list abc seq 10 deny 10.0.0.0/8 le 32
!
```

Related Commands

Command	Description
clear configure prefix-list	Clears the **prefix-list** commands from the running configuration.

show running-config priority-queue

To display the priority queue configuration details for an interface, use the **show running-config priority-queue** command in privileged EXEC mode.

show running-config priority-queue *interface-name*

Syntax Description

interface-name	Specifies the name of the interface for which you want to show the priority queue details

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows the use of the show running-config priority-queue command for the interface named test, and the command output:

```
hostname# show running-config priority-queue test
priority-queue test
  queue-limit   50
  tx-ring-limit 10
hostname#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the statistics for the priority queue configured on the named interface.

show running-config privilege

To display the privileges for a command or a set of commands, use the **show running-config privilege** command in privileged EXEC mode.

show running-config [all] privilege [**all** | **command** *command* | **level** *level*]

Syntax Description

all	(Optional) First occurrence -- Displays the default privilege level.
all	(Optional) Second occurrence -- Displays the privilege level for all commands.
command *command*	(Optional) Displays the privilege level for a specific command.
level *level*	(Optional) Displays the commands that are configured with the specified level; valid values are from 0 to 15.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified for this release to conform to CLI guidelines.

Usage Guidelines

Use the **show running-config privilege** command to view the current privilege level.

Examples

```
hostname(config)# show running-config privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
privilege	Configure the command privilege levels.
show curpriv	Display current privilege level.
show running-config privilege	Display privilege levels for commands.

show running-config regex

To display all regular expressions configured with the **regex** command, use the **show running-config regex** command in privileged EXEC mode.

show running-config regex

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output of the **show running-config regex** command, which shows all regular expressions:

```
hostname# show running-config regex
regex test "string"
```

Related Commands

Command	Description
class-map type regex	Creates a regular expression class map.
clear configure regex	Clears all regular expressions.
regex	Creates a regular expression.
test regex	Tests a regular expression.

show running-config route

To display the route configuration that is running on the security appliance, use the **show running-config route** command in privileged EXEC mode.

show running-config [**all**] **route**

Syntax Description

No default behavior or values.

Defaults

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config route** command:

```
hostname# show running-config route
route outside 10.30.10.0 255.255.255.0 1
```

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Specifies a static or default route for the an interface.
show route	Displays route information.

show running-config route-map

To display the information about the route map configuration, use the **show running-config route-map** command in privileged EXEC mode.

show running-config route-map [*map_tag*]

Syntax Description

map_tag	(Optional) Text for the route-map tag.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0(1)	Added keyword **running-config**.

Usage Guidelines

To show all route-maps defined in the configuration, use the **show running-config route-map** command. To show individual route-maps by name, use the **show running-config route-map** *map_tag* command, where *map_tag* is the name of the route-map. Multiple route maps may share the same map tag name.

Examples

The following is sample output from the **show running-config route-map** command:

```
hostname# show running-config route-map
route-map maptag1 permit sequence 10
    set metric 5
    match metric 3
route-map maptag1 permit sequence 12
    set metric 5
    match interface backup
    match metric 3
route-map maptag2 deny sequence 10
    match interface dmz
```

Related Commands

Command	Description
clear configure route-map	Removes the conditions for redistributing the routes from one routing protocol into another routing protocol.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

show running-config router

To display the global configuration commands for the specified routing protocol, use the **show running-config router** command in privileged EXEC mode.

show running-config [all] **router** [**ospf** [*process_id*] | **rip** | **eigrp** [*as-number*]]

Syntax Description

all	Shows all router commands, including the commands you have not changed from the default.
as-number	(Optional) Displays the router configuration commands for the specified EIGRP autonomous system number. If not specified, the router configuration commands for all EIGRP routing processes are displayed. Because only one EIGRP routing process is supported on the security appliance, including the optional *as-number* argument has the same effect as omitting it.
eigrp	(Optional) Displays the EIGRP router configuration commands.
ospf	(Optional) Displays the OSPF router configuration commands.
process_id	(Optional) Displays the commands for the selected OSPF process.
rip	(Optional) Displays the RIP router configuration commands.

Defaults

If a routing protocol is not specified, the router configuration commands for all configured routing protocols are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show router** command to the **show running-config router** command.
8.0(2)	This command was modified to include the **eigrp** keyword.

Examples

The following is sample output from the **show running-config router ospf** command:

```
hostname# show running-config router ospf 1

router ospf 1
  log-adj-changes detail
  ignore lsa mospf
  no compatible rfc1583
```

```
  distance ospf external 200
  timers spf 10 20
  timers lsa-group-pacing 60
```

The following is sample output from the **show running-config router rip** command:

```
hostname# show running-config router rip

router rip
    network 10.0.0.0
    version 2
    no auto-summary
```

Related Commands

Command	Description
clear configure router	Clears all router commands from the running configuration.
router eigrp	Enables an EIGRP routing process and enters router configuration mode for that process.
router ospf	Enables an OSPF routing process and enters router configuration mode for that process.
router rip	Enables a RIP routing process and enters router configuration mode for that process.

show running-config same-security-traffic

To display the same-security interface communication, use the **show running-config same-security-traffic** command in privileged EXEC mode.

show running-config same-security-traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config same-security-traffic** command:

```
hostname# show running-config same-security-traffic
```

Related Commands

Command	Description
same-security-traffic	Permits communication between interfaces with equal security levels.

show running-config service

To display the system services, use the **show running-config service** command in privileged EXEC mode.

show running-config service

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **running-config** was added.

Examples

This command shows how to display the system services:

```
hostname# show running-config service
service resetoutside
```

Related Commands

Command	Description
service	Enables system services.

show running-config service-policy

To display all currently running service policy configurations, use the **show runnig-config service-policy** command in privileged EXEC mode.

show running-config [all] service-policy

Syntax Description

all	(Optional) Shows all service policy commands, including the commands you have not changed from the default.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output of the **show running-config service-policy** command:

```
hostname# show running-config service-policy
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
service-policy	Configures service policies.
clear service-policy	Clears service policy configurations.
clear configure service-policy	Clears service policy configurations.

show running-config sla monitor

To display the SLA operation commands in the running configuration, use the **show running-config sla monitor** command in privileged EXEC mode.

show running-config sla monitor [*sla-id*]

Syntax Description

sla_id	Specifies the SLA ID for the **sla monitor** commands being displayed. Valid values are from 1 to 2147483647.

Defaults

If the *sla-id* is not specified, the **sla monitor** commands for all SLA operations are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command displays the **sla monitor** commands, associated SLA monitor configuration mode commands, and the associated **sla monitor** schedule command, if present. It does not display the **track rtr** commands in the configuration.

Examples

The following is sample output from the **show running-config sla monitor 5** command. It displays the SLA monitor configuration for the SLA operation with the SLA ID of 5:

```
hostname# show running-config sla monitor 5

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

Related Commands

Command	Description
clear configure sla monitor	Removes the **sla monitor**, and associated commands, from the running configuration.
show sla monitor configuration	Displays configuration values for the specified SLA operation.

show running-config smtps

To display the running configuration for smpts, use the s**how running-config smtps** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] smtps

Syntax Description

all	Displays the running configuration including default values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config smtps** command:

```
hostname# show running-config smtps

smtps
server 10.1.1.21
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all smtps

smtps
 port 995
 server 10.1.1.21
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
hostname#
```

ASA-4#

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
smtps	Creates or edits an SMTPS e-mail proxy configuration

show running-config snmp-map

To show the SNMP maps that have been configured, use the **show running-config snmp-map** command in privileged EXEC mode.

show running-config snmp-map *map_name*

Syntax Description.

map_name	Displays the configuration for the specified SNMP map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config snmp-map** command displays the SNMP maps that have been configured.

Examples

The following is sample output from the **show running-config snmp-map** command:

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enables SNMP application inspection.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.

show running-config snmp-server

To display all currently running SNMP server configurations, use the **show runnig-config snmp-server** command in global configuration mode.

show running-config [default] snmp-server

Syntax Description

default	Displays the default SNMP server configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is an example of the **show running-config snmp-server** command:

```
hostname# show running-config snmp-server
snmp-server host inside 10.21.104.209 community asa1
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

Related Commandsh

Command	Description
snmp-server	Configures the SNMP server.
clear snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays the SNMP server configuration.

show running-config ssh

To show the SSH commands in the current configuration, use the **show running-config ssh** command in privileged EXEC mode.

show running-config [**default**] **ssh** [**timeout** | **version**]

show run [**default**] **ssh** [**timeout**]

Syntax Description

default	(Optional) Displays the default SSH configuration values along with the configured values.
timeout	(Optional) Displays the current SSH session timeout value.
version	(Optional) Displays the version of SSH currently being supported.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The command was changed from the **show ssh** command to the **show running-config ssh** command.

Usage Guidelines

This command shows the current ssh configuration. To display only the SSH session timeout value, use the **timeout** option. To see a list of active SSH sessions, use the **show ssh sessions** command.

Examples

The following example displays the SSH session timeout:

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

show running-config ssl

To display the current set of configured ssl commands, use the **show running-config ssl** command in privileged EXEC mode.

show running-config ssl

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the `show running-config ssl` command:

```
hostname# show running-config ssl
ssl server-version  tlsv1
ssl client-version tlsv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

show running-config static

To display all **static** commands in the configuration, use the **show running-config static** command in privileged EXEC mode.

show running-config static

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **running-config** was added.

Usage Guidelines

This command displays the maximum connections value for the UDP protocol. If the UDP maximum connections value is “0” or not set, the limit enforcement is disabled.

Examples

This example shows how to display all static commands in the configuration:

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```

Note No UDP value connection limit is shown.

Related Commands

Command	Description
clear configure static	Removes all the **static** commands from the configuration.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

show running-config sunrpc-server

To display the information about the SunRPC configuration, use the **show running-config sunrpc-server** command in privileged EXEC mode.

show running-config sunrpc-server *interface_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [- *port*] **timeout** *hh:mm:ss*

Syntax Description

interface_name	Server interface.
ip_addr	Server IP address.
mask	Network mask.
port *port - port*	SunRPC protocol port range and optionally, a second port.
protocol	SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program type.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.
TCP	(Optional) Specifies TCP.
UDP	(Optional) Specifies UDP.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The *service_type* is specified in the **sunrpcinfo** command.

Examples

The following is sample output from the **show running-config sunrpc-server** command:

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the SunRPC services from the security appliance.
debug sunrpc	Enables debug information for SunRPC.
show conn	Displays the connection state for different connection types, including SunRPC.
sunrpc-server	Creates the SunRPC services table.
timeout	Sets the maximum idle time duration for different protocols and session types, including SunRPC.

show running-config sysopt

To show the **sysopt** command configuration in the running configuration, use the **show running-config sysopt** command in privileged EXEC mode.

show running-config sysopt

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show sysopt** command.

Examples

The following is sample output from the **show running-config sysopt** command:

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

show running-config tcp-map

To display the information about the TCP map configuration, use the **show running-config tcp-map** command in privileged EXEC mode.

show running-config tcp-map [*tcp_map_name*]

Syntax Description

tcp_map_name	(Optional) Text for the TCP map name; the text can be up to 58 characters in length.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config tcp-map** command:

```
hostname# show running-config tcp-map
tcp-map localmap
```

Related Commands

Command	Description
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.
clear configure tcp-map	Clears the TCP map configuration.

show running-config telnet

To display the current list of IP addresses that are authorized to use Telnet connections to the security appliance, use the **show running-config telnet** command in privileged EXEC mode. You can also use this command to display the number of minutes that a Telnet session can remain idle before being closed by the security appliance.

show running-config telnet [**timeout**]

Syntax Description

timeout	(Optional) Displays the number of minutes that a Telnet session can be idle before being closed by the security appliance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The keyword **running-config** was added.

Examples

This example shows how to display the current list of IP addresses that are authorized for use by Telnet connections to the security appliance:

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

Related Commands

Command	Description
clear configure telnet	Removes the Telnet connection from the configuration.
telnet	Adds Telnet access to the console and sets the idle timeout.

show running-config terminal

To display the current terminal settings, use the **show running-config terminal** command in privileged EXEC mode.

show running-config terminal

Syntax Description

This command has no keywords or arguments.

Defaults

The default display width is 80 columns.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example clears the page length setting:

```
hostname# show running-config terminal

Width = 80, no monitor
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
terminal	Sets the terminal line parameters.
terminal width	Sets the terminal display width.

show running-config tftp-server

To display the default TFTP server address and directory, use the **show running-config tftp-server** command in global configuration mode.

show running-config tftp-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The **running-config** keyword was added.

Examples

This example shows how to display the IP/IPv6 address of the default TFTP server and the directory of the configuration file:

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

Related Commands

Command	Description
configure net	Loads the configuration from the TFTP server and path you specify.
tftp-server	Configures the default TFTP server address and the directory of the configuration file.

show running-config threat-detection

To view the threat detection configuration, use the **show running-config threat-detection** command in privileged EXEC mode.

show running-config [**all**] **threat-detection** [**basic-threat** | **rate** | **scanning-threat** | **statistics** [**tcp-intercept**]]

Syntax Description

all	(Optional) Shows all threat detection commands, including the commands you have not changed from the default. For example, you can view the default rate limits for the **threat-detection basic-threat** command.
basic-threat	(Optional) Shows the basic threat configuration.
rate	(Optional) Shows the rate configuration.
scanning-threat	(Optional) Shows the scanning threat configuration.
statistics	(Optional) Shows the statistics configuration.
tcp-intercept	(Optional) Shows the statistics configuration for TCP Intercept.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The **tcp-intercept** keyword was added.

Examples

The following is sample output from the **show running-config all threat-detection** command, which shows the default rate limits for the **threat-detection basic-threat** command:

```
hostname# show running-config all threat-detection
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 400 burst-rate 800
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
```

```
threat-detection rate icmp-drop rate-interval 3600 average-rate 100 burst-rate 400
threat-detection rate scanning-drop rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-drop rate-interval 3600 average-rate 5 burst-rate 10
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 100 burst-rate 200
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 400 burst-rate 1600
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 2000 burst-rate 8000
threat-detection scanning-threat shun duration 3600
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

show running-config timeout

To display the timeout value of all protocols, or just a specific one, use the **show running-config timeout** command in privileged EXEC mode.

show running-config timeout *protocol*

Syntax Description

protocol	(Optional) Displays the timeout value of the specified protocol. Supported protocols are: **xlate**, **conn, udp**, **icmp**, **rpc**, **h323**, **h225**, **mgcp**, **mgcp-pat**, **sip**, **sip_media**, and **uauth**.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The **running-config** and **mgcp-pat** keywords were added.

Examples

This example shows how to display the timeout values for the system:

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

Related Commands

Command	Description
clear configure timeout	Restores the default idle time durations.
timeout	Sets the maximum idle time duration.

show running-config tls-proxy

To display all currently running TLS proxy configurations, use the **show running-config tls-proxy** command in privileged EXEC mode.

show running-config [**all**] **tls-proxy** [*proxy_name*]

Syntax Description

all	Shows all TLS proxy commands, including the commands you have not changed from the default.
proxy_name	Specifies the name of the TLS proxy to show.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following is sample output of the **show running-config all tls-proxy** command:

```
hostname# show running-config tls-proxy
tls-proxy proxy
    server trust-point local_ccm
    client ldc issuer ldc_signer
    client ldc key-pair phone_common
    no client cipher-suite
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows all TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show running-config track

To display **track rtr** commands in the running configuration, use the **show running-config track** command in privileged EXEC mode.

show running-config track [*track-id*]

Syntax Description

track-id	(Optional) Limits the display to the **track rtr** command with the specified tracking object ID.

Defaults

If the *track-id* is not specified, all **track rtr** commands in the running configuration are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show running-config track** command:

```
hostname# show running-config track 5

track 5 rtr 124 reachability
```

Related Commands

Command	Description
clear configure track	Removes the **track rtr** commands from the running configuration.
show track	Displays information about the objects being tracked.
track rtr	Creates a tracking entry to poll the SLA.

show running-config tunnel-group

To display tunnel group information about all or a specified tunnel group and tunnel-group attributes, use the **show running-config tunnel-group** command in global configuration or privileged EXEC mode.

show running-config [**all**] **tunnel-group** [*name* [**general-attributes | ipsec-attributes | ppp-attributes**]]

Syntax Description

all	[Optional] Displays all tunnel-group commands, including the commands you have not changed from the default.
general-attributes	Displays configuration information for general attributes.
ipsec-attributes	Displays configuration information for IPSec attributes.
name	Specifies the name of the tunnel group.
ppp-attributes	Displays configuration information for PPP attributes.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•		•		
Privileged EXEC	•		•		

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays the current configuration for all tunnel groups:

```
hostname<config># show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname<config>#
```

Related Commands

Command	Description
clear configure tunnel-group	Removes tunnel-group configuration
tunnel-group general-attributes	Enters subconfiguration mode for specifying general attributes for specified tunnel group.
tunnel-group ipsec-attributes	Enters subconfiguration mode for specifying IPSec attributes for specified tunnel group.
tunnel-group	Enters tunnel-group subconfiguration mode for the specified type.

show running-config url-block

To show the configuration for buffers and memory allocation used by URL filtering, use the **show running-config url-block** command in privileged EXEC mode.

show running-config url-block [**block** | **url-mempool** | **url-size**]

Syntax Description

block	Displays the configuration for the maximum number of blocks that will be buffered.
url-mempool	Displays the configuration for the maximum allow URL size (in KB).
url-size	Displays the configuration for the memory resource (in KB) allocated for the long URL buffer.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Prexisting	This command was previously existing.

Usage Guidelines

The **show running-config url-block** command displays the configuration for buffers and memory allocation used by URL filtering.

Examples

The following is sample output from the **show running-config url-block** command:

```
hostname# show running-config url-block
!
url-block block 56
!
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-config url-cache

To show the cache configuration used by URL filtering, use the **show running-config url-cache** command in privileged EXEC mode.

show running-config url-cache

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was previously existing.

Usage Guidelines

The **show running-config url-cache** command displays the cache configuration used by URL filtering.

Examples

The following is sample output from the **show running-config url-cache** command:

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-config url-server

To show the URL filtering server configuration, use the **show running-config url-server** command in privileged EXEC mode.

show running-config url-server

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was previously existing.

Usage Guidelines

The **show running-config url-server** command displays the URL filtering server configuration.

Examples

The following is sample output from the **show running-config url-server** command:

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-config username

To display the running configuration for a particular user, use the **show running-config username** command in privileged EXEC mode with the username appended. To display the running configuration for all users, use this command without a username.

show running-config [**all**] **username** [*name*] [**attributes**]]

Syntax Description

attributes	Displays the specific AVPs for the user(s)
all	(Optional) Displays all username commands, including the commands you have not changed from the default.
name	Provides the name of the user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the show the running-config username for a user named anyuser:

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

Related Commands

Command	Description
clear config username	Clears the username database.
username	Adds a user to the security appliance database.
username attributes	Lets you configure attributes for specific users.

show running-config virtual

To display the IP address of the security appliance virtual server, use the **show running-config virtual** command in privileged EXEC mode.

show running-config [**all**] **virtual**

Syntax Description

all	Display the virtual server IP address of all virtual servers.

Defaults

Omitting the **all** keyword displays the explicitly configured IP address of the current virtual server or servers.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

You must be in privileged EXEC mode to use this command.

Examples

This example displays the **show running-config virtual** command output for a situation in which there is a previously configured HTTP virtual server:

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
virtual	Displays the address for authentication virtual servers.

show running-config vpn load-balancing

To display the current VPN load-balancing virtual cluster configuration, use the **show running-config vpn-load-balancing** command in global configuration, privileged EXEC or VPN load-balancing mode.

show running-config [**all**] **vpn load-balancing**

Syntax Description

all	Display both the default and the explicitly configured VPN load-balancing configuration.

Defaults

Omitting the **all** keyword displays the explicitly configured VPN load-balancing configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show running-config vpn load-balancing** command also displays configuration information for the following related commands: **cluster encryption**, **cluster ip address**, **cluster key**, **cluster port**, **nat**, **participate**, and **priority**.

Examples

This example displays **show running-config vpn load-balancing** command and its output, with the **all** option enabled:

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
 no nat
 priority 9
 interface lbpublic test
 interface lbprivate inside
 no cluster ip address
 no cluster encryption
 cluster port 9023
 no participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show vpn load-balancing	Displays the VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

show running-config webvpn

To display the running configuration for webvpn, use the s**how running-config webvpn** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] webvpn [apcf | auto-signon | cache | proxy-bypass | rewrite | sso-server | url-list]

Syntax Description

all	(Optional) Displays the running configuration including default values.
apcf	(Optional) Displays the running configuration for SSL VPN APCF.
auto-signon	(Optional) Displays the running configuration for SSL VPN auto sign-on.
cache	(Optional) Displays the running configuration for SSL VPN caching.
proxy-bypass	(Optional) Displays the running configuration for SSL VPN proxy bypass.
rewrite	(Optional) Displays the running configuration for SSL VPN content transformation.
sso-server	(Optional) Displays the running configuration for single sign-on.
url-list	(Optional) Displays the running configuration for SSL VPN access to URLs.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was revised.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—
WebVPN	•	—	•	—	—

Examples

The following is sample output from the **show running-config webvpn** command:

```
hostname# show running-configuration webvpn
webvpn
 title WebVPN Services for ASA-4
 title-color green
 default-idle-timeout 0
 nbns-server 10.148.1.28 master timeout 2 retry 2
```

```
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 authorization-dn-attributes CN
```

The following is sample output from the **show running-config all webvpn** command:

```
hostname#(config-webvpn)# show running-config all webvpn

webvpn
 title WebVPN Services for ASA-4
 username-prompt Username
 password-prompt Password
 login-message Please enter your username and password
 logout-message Goodbye
 no logo
 title-color green
 secondary-color #CCCCFF
 text-color white
 secondary-text-color black
 default-idle-timeout 0
 no http-proxy
 no https-proxy
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 no authorization-server-group
 default-group-policy DfltGrpPolicy
 authentication aaa
 no authorization-required
 authorization-dn-attributes CN
hostname#
```

The following is sample output from the **show running-config webvpn sso-server** command:

```
hostname#(config-webvpn)# show running-config webvpn sso-server
sso-server
sso-server bxbsvr type siteminder
web-agent-url http://bxb-netegrity.demo.com/vpnauth/
policy-server-secret cisco1234
sso-server policysvr type siteminder
web-agent-url http://webagent1.mysiteminder.com/ciscoauth/
policy-server-secret Cisco1234
max-retry-attempts 4
request-timeout 10
hostname#(config-webvpn)#
```

Related Commands

Command	Description
clear configure webvpn	Removes all nondefault SSL VPN configuration attributes.
debug webvpn	Displays debug information about SSL VPN sessions.
show webvpn	Displays statistics about SSL VPN sessions.

show running-config webvpn auto-signon

To display all WebVPN auto-signon assignments in the running configuration, use the **show running-config webvpn auto-signon** command in global configuration mode.

show running-config webvpn auto-signon

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config webvpn auto-signon**:

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
hostname(config-webvpn)# auto-signon allow uri *.example.com/* auth-type basic
hostname(config-webvpn)# show running-config webvpn auto-signon
auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
auto-signon allow uri *.example.com/* auth-type basic
```

Related Commands

auto-signon	Configures the security appliance to automatically pass WebVPN login credentials to internal servers.

show running-config zonelabs-integrity

To display the Zone Labs Integrity Server configuration, use the **show running-config zonelabs-integrity** command in privileged EXEC mode.

show running-config [**all**] **zonelabs-integrity**

Syntax Description

all	(Optional) Shows the running configuration including default configuration values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command to display the addresses of all Zone Labs Integrity Servers and the configured values for the active Zone Labs Integrity Server. Use the **all** parameter to display the default as well as the explicitly configured values.

Examples

The following is sample output from the **show running-config zonelabs-integrity** command:

```
hostname# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
hostname#
```

The following is sample output from the **show running-config all zonelabs-integrity** command:

```
hostname# show running-config all zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
zonelabs-integrity interface none
zonelabs-integrity fail-open
zonelabs-integrity fail-timeout 10
zonelabs-integrity ssl-client-authentication disable
zonelabs-integrity ssl-certificate-port 80
hostname#
```

Related Commands

Command	Description
clear configure zonelabs-integrity	Clears the Zone Labs Integrity Server configuration.

show running-config vpdn

To display the VPDN configuration used for PPPoE connections, use the **show running-config vpdn** command in privileged EXEC mode:

show running-config vpdn

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

This example shows the use of the show running-config vpdn command and the command output:

```
hostname# show running-config vpdn
vpdn group telecommuters ppp authentication mschap
vpdn username tomm password ********* store-local
```

Related Commands

Command	Description
show running-config vpdn group	Shows the current configuration for vpdn group.
show running-config vpdn username	Shows the current configuration for vpdn usernames.

show running-configuration vpn-sessiondb

To display the current set of configured vpnsessiondb commands, use the **show running-configuration vpn-sessiondb** command in privileged EXEC mode.

show running-configuration [all] vpn-sessiondb

Syntax Description

all	(Optional) Displays all **vpn-sessionddb** commands, including the commands you have not changed from the default

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

As of Release 7.0, this command displays only the VPN maximum sessions limit, if configured.

Examples

The following is sample output for the **show running-configuration vpn-sessiondb** command:

```
hostname# show running-configuration vpn-sessiondb
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show running-config wccp

To show the WCCP configuration in the running configuration, use the **show running-config wccp** command in privileged EXEC mode.

show [**all**] **running-config wccp**

Syntax Description

all	Displays the default and explicitly configured configuration information for one or all WCCP commands.

Defaults

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show running-config wccp** command:

```
hostname# show running-config wccp
wccp web-cache redirect-list wooster group-list jeeves password whatho
hostname#
```

Related Commands

Command	Description
wccp	Enables support of WCCP.
wccp redirect	Enters support of WCCP redirection.

CHAPTER 30

show service-policy through show xlate Commands

show service-policy

To display the service policy statistics, use the **show service-policy** command in privileged EXEC mode.

show service-policy [**global** | **interface** *intf*] [**csc** | **inspect** | **ips** | **police** | **priority | shape**]

show service-policy [**global** | **interface** *intf*] [**set connection** [**details**]]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

csc	(Optional) Limits the output to policies that include the **csc** command.
dest_ip dest_mask	The destination IP address and netmask of the traffic flow.
details	(Optional) Displays per-client connection information, if a per-client connection limit is enabled.
eq *dest_port*	(Optional) The equals operator, requiring the destination port to match the port number that follows.
eq *src_port*	(Optional) The equals operator, requiring the source port to match the port number that follows.
flow *protocol*	(Optional) Specifies a traffic flow for which you want to see the policies that the security appliance would apply to the flow. The arguments and keywords following the **flow** keyword specify the flow in ip-5-tuple format. Valid values for the *protocol* argument are listed in the "Usage Guidelines" section, below.
global	(Optional) Limits output to the global policy, which applies to all interfaces.
host *dest_host*	The host destination IP address of the traffic flow.
host *src_host*	The host source IP address of the traffic flow.
icmp_control_message	(Optional) Specifies an ICMP control message of the traffic flow. Valid values for the *icmp_control_message* argument are listed in the "Usage Guidelines" section, below.
icmp_number	(Optional) Specifies the ICMP protocol number of the traffic flow.
inspect	(Optional) Limits the output to policies that include an **inspect** command.
interface *intf*	(Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name given by the **nameif** command.
ips	Limits output to policies that include the **ips** command.
police	Limits output to policies that include the **police** command.
priority	Limits output to policies that include the **priority** command.
set connection	Limits output to policies that include the **set connection** command.
shape	Limits output to policies that include the **shape** command.
src_ip src_mask	The source IP address and netmask used in the traffic flow.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **csc** keyword was added.
7.2(4)/8.0(4)	The **shape** keyword was added.

Usage Guidelines

The **flow** keyword lets you determine, for any flow that you can describe, the policies that the security appliance would apply to that flow. You can use this to check that your service policy configuration will provide the services you want for specific connections. The arguments and keywords following the **flow** keyword specifies the flow in ip-5-tuple format with no object grouping.

Because the flow is described in ip-5-tuple format, not all match criteria are supported. Following are the list of match criteria that are supported for flow match:

- **match access-list**
- **match port**
- **match rtp**
- **match default-inspection-traffic**

The **priority** keyword is used to display the aggregate counter values of packets transmitted through an interface.

The number of embryonic connections displayed in the **show service-policy** command output indicates the current number of embryonic connections to an interface for traffic matching that defined by the **class-map** command. The “embryonic-conn-max” field shows the maximum embryonic limit configured for the traffic class using the Modular Policy Framework. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic type defined by the **class-map** command.

protocol Argument Values

The following are valid values for the *protocol* argument:

- *number*—The protocol number (0 - 255).
- **ah**
- **eigrp**
- **esp**
- **gre**
- **icmp**
- **icmp6**
- **igmp**

- **igrp**
- **ip**
- **ipinip**
- **ipsec**
- **nos**
- **ospf**
- **pcp**
- **pim**
- **pptp**
- **snp**
- **tcp**
- **udp**

icmp_control_message Argument Values

The following are valid values for the *icmp_control_message* argument:

- **alternate-address**
- **conversion-error**
- **echo**
- **echo-reply**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **parameter-problem**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **unreachable**

Examples

The following is sample output from the **show service-policy global** command:

```
hostname# show service-policy global

Global policy:
```

```
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

The following is sample output from the **show service-policy priority** command:

```
hostname# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

The following is sample output from the **show service-policy flow** command:

```
hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

The following is sample output from the **show service-policy inspect http** command. This example shows the statistics of each match command in a match-any class map.

```
hostname# show service-policy inspect http

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

The following is sample output from the **show service-policy inspect waas** command. This example shows the waas statistics.

```
hostname# show service-policy inspect waas

Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
       SYN with WAAS option 4
       SYN-ACK with WAAS option 4
       Confirmed WAAS connections 4
       Invalid ACKs seen on WAAS connections 0
       Data exceeding window size on WAAS connections 0
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears all service policy configurations.
service-policy	Configures the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.

show service-policy inspect gtp

To display the GTP configuration, use the **show service-policy inspect gtp** command in privileged EXEC mode.

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **pdpmcb** | **requests** | **statistics** [**gsn** *IP_address*] }

Syntax Description.

apn	(Optional) Displays the detailed output of the PDP contexts based on the APN specified.
ap_name	Identifies the specific access point name for which statistics are displayed.
detail	(Optional) Displays the detailed output of the PDP contexts.
imsi	Displays the detailed output of the PDP contexts based on the IMSI specified.
IMSI_value	Hexadecimal value that identifies the specific IMSI for which statistics are displayed.
interface	(Optional) Identifies a specific interface.
int	Identifies the interface for which information will be displayed.
gsn	(Optional) Identifies the GPRS support node, which is interface between the GPRS wireless data network and other networks.
gtp	(Optional) Displays the service policy for GTP.
IP_address	IP address for which statistics are displayed.
ms-addr	(Optional) Displays the detailed output of the PDP contexts based on the MS Address specified.
pdp-context	(Optional) Identifies the Packet Data Protocol context
pdpmcb	(Optional) Displays the status of the PDP master control block.
requests	(Optional) Displays status of GTP requests.
statistics	(Optional) Displays GTP statistics.
tid	(Optional) Displays the detailed output of the PDP contexts based on the TID specified.
tunnel_ID	Hexadecimal value that identifies the specific tunnel for which statistics are displayed.
version	(Optional) Displays the detailed output of the PDP contexts based on the GTP version.
version_num	Specifies the version of the PDP context for which statistics are displayed. The valid range is 0 to 255.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can use the vertical bar | to filter the display. Type | for more display filtering options.

The **show pdp-context** command displays PDP context-related information.

The Packet Data Protocol context is identified by the tunnel ID, which is a combination of IMSI and NSAPI. A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station user.

The **show gtp requests** command displays current requests in the request queue.

Examples

The following is sample output from the **show gtp requests** command:

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

You can use the vertical bar | to filter the display, as in the following example:

```
hostname# show service-policy gtp statistics | grep gsn
```

This example shows the GTP statistics with the word gsn in the output.

The following command shows the statistics for GTP inspection:

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

The following command displays information about the PDP contexts:

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

Table 30-1 describes each column the output from the **show service-policy inspect gtp pdp-context** command.

Table 30-1 PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr	Displays the serving gateway service node.
Idle	Displays the time for which the PDP context has not been in use.
APN	Displays the access point name.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.

show service-policy inspect radius-accounting

To display the GTP configuration, use the **show service-policy inspect radius-accounting** command in privileged EXEC mode.

show service-policy [**interface** *int*] **inspect radius-accounting**

Syntax Description.

interface *int*	(Optional) Identifies a specific interface.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show gtp requests** command:

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

You can use the vertical bar | to filter the display, as in the following example:

```
hostname# show service-policy gtp statistics | grep gsn
```

This example shows the GTP statistics with the word gsn in the output.

The following command shows the statistics for GTP inspection:

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

The following command displays information about the PDP contexts:

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

Table 30-1 describes each column the output from the **show service-policy inspect gtp pdp-context** command.

Table 30-2 PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr	Displays the serving gateway service node.
Idle	Displays the time for which the PDP context has not been in use.
APN	Displays the access point name.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.

show shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | *statistics*]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface counters only.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show shun** command:

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.

show sip

To display SIP sessions, use the **show sip** command in privileged EXEC mode.

show sip

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show sip** command assists in troubleshooting SIP inspection engine issues and is described with the **inspect protocol sip udp 5060** command. The **show timeout sip** command displays the timeout value of the designated protocol.

The **show sip** command displays information for SIP sessions established across the security appliance. Along with the **debug sip** and **show local-host** commands, this command is used for troubleshooting SIP inspection engine issues.

Note We recommend that you configure the **pager** command before using the **show sip** command. If there are a lot of SIP session records and the **pager** command is not configured, it will take a while for the **show sip** command output to reach its end.

Examples

The following is sample output from the **show sip** command:

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the security appliance (as shown in the `Total` field). Each `call-id` represents a call.

The first session, with the `call-id c3943000-960ca-2e43-228f@10.130.56.44,` is in the state `Call Init`, which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state `Active`, in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug sip	Enables debug information for SIP.
inspect sip	Enables SIP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show skinny

To troubleshoot SCCP (Skinny) inspection engine issues, use the **show skinny** command in privileged EXEC mode.

show skinny

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show skinny** command assists in troubleshooting SCCP (Skinny) inspection engine issues.

Examples

The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the security appliance. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco CallManager at 172.18.1.33. TCP port 2000 is the CallManager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco CallManager.

```
hostname# show skinny

        LOCAL                   FOREIGN                 STATE

-----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

The following is the xlate information for these Skinny connections:

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debug information.
inspect skinny	Enables SCCP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show sla monitor configuration

To display the configuration values, including the defaults, for SLA operations, use the **show sla monitor configuration** command in user EXEC mode.

show sla monitor configuration [*sla-id*]

Syntax Description

sla-id	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Defaults

If the *sla-id* is not specified, the configuration values for all SLA operations are shown.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **show running config sla monitor** command to see the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor** command. It displays the configuration values for SLA operation 123. Following the output of the **show sla monitor** command is the output of the **show running-config sla monitor** command for the same SLA operation.

```
hostname> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
```

```
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

hostname# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show sla monitor operational-state

To display the operational state of SLA operations, use the **show sla monitor operational-state** command in user EXEC mode.

show sla monitor operational-state [*sla-id*]

Syntax Description

sla-id	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Defaults

If the *sla-id* is not specified, statistics for all SLA operations are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **show running-config sla monitor** command to display the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor operational-state** command:

```
hostname> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
```

```
NumOfRTT: 0      RTTSum: 0        RTTSum2: 0
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show snmp-server statistics

To display SNMP server statistics, use the **show snmp-server statistics** command in privileged EXEC mode.

show snmp-server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

This example shows how to display the SNMP server statistics:

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

Related Commands

Command	Description
snmp-server	Provides the security appliance event information through SNMP.
clear configure snmp-server	Disables the SNMP server.
show running-config snmp-server	Displays the SNMP server configuration.

show ssh sessions

To display information about the active SSH session on the security appliance, use the **show ssh sessions** command in privileged EXEC mode.

show ssh sessions [*ip_address*]

Syntax Description

ip_address	(Optional) Displays session information for only the specified IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The SID is a unique number that identifies the SSH session. The Client IP is the IP address of the system running an SSH client. The Version is the protocol version number that the SSH client supports. If the SSH only supports SSH version 1, then the Version column displays 1.5. If the SSH client supports both SSH version 1 and SSH version 2, then the Version column displays 1.99. If the SSH client only supports SSH version 2, then the Version column displays 2.0. The Encryption column shows the type of encryption that the SSH client is using. The State column shows the progress that the client is making as it interacts with the security appliance. The Username column lists the login username that has been authenticated for the session.

Examples

The following example demonstrates the output of the **show ssh sessions** command:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

Related Commands

Command	Description
ssh disconnect	Disconnects an active SSH session.
ssh timeout	Sets the timeout value for idle SSH sessions.

show startup-config

To show the startup configuration or to show any errors when the startup configuration loaded, use the **show startup-config** command in privileged EXEC mode.

show startup-config [errors]

Syntax Description

errors	(Optional) Shows any errors that were generated when the security appliance loaded the startup configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System[1]
Privileged EXEC	•	•	•	•	•

1. The **errors** keyword is only available in single mode and the system execution space,

Command History

Release	Modification
7.0(1)	The **errors** keyword was added.

Usage Guidelines

In multiple context mode, this command shows the startup configuration for your current execution space: the system configuration or the security context.

To clear the startup errors from memory, use the **clear startup-config errors** command.

Examples

The following is sample output from the **show startup-config** command:

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
```

```
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

The following is sample output from the **show startup-config errors** command:

```
hostname# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "  limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', " nameif inside"
.....
*** Output from config line 37, "  config-url disk:/admin..."
```

Related Commands

Command	Description
clear startup-config errors	Clears the startup errors from memory.
show running-config	Shows the running configuration.

show sunrpc-server active

To display the pinholes open for Sun RPC services, use the **show sunrpc-server active** command in privileged EXEC mode.

show sunrpc-server active

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Use the **show sunrpc-server active** command to display the pinholes open for Sun RPC services, such as NFS and NIS.

Examples

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. The following is sample output from the **show sunrpc-server active** command:

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
clear sunrpc-server active	Clears the pinholes opened for Sun RPC services, such as NFS or NIS.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.

show switch mac-address-table

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **show switch mac-address-table** command in privileged EXEC mode to view the switch MAC address table.

show switch mac-address-table

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is for models with built-in switches only. The switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN in the switch hardware. If you are in transparent firewall mode, use the **show mac-address-table** command to view the bridge MAC address table in the ASA software. The bridge MAC address table maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

MAC address entries age out in 5 minutes.

Examples

The following is sample output from the **show switch mac-address-table** command.

```
hostname# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

Table 30-3 shows each field description:

Table 30-3 show switch mac-address-table Fields

Field	Description
Mac Address	Shows the MAC address.
VLAN	Shows the VLAN associated with the MAC address.
Type	Shows if the MAC address was learned dynamically, as a static multicast address, or statically. The only static entry is for the internal backplane interface.
Age	Shows the age of a dynamic entry in the MAC address table.
Port	Shows the switch port through which the host with the MAC address can be reached.

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table for models that do not have a built-in switch.
show switch vlan	Shows the VLAN and physical MAC address association.

show switch vlan

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **show switch vlan** command in privileged EXEC mode to view the VLANs and the associated switch ports.

show switch vlan

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is for models with built-in switches only. For other models, use the **show vlan** command.

Examples

The following is sample output from the **show switch vlan** command.

```
hostname# show switch vlan

VLAN Name                            Status    Ports
---- ------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

Table 30-3 shows each field description:

Table 30-4 show switch vlan Fields

Field	Description
VLAN	Shows the VLAN number.
Name	Shows the name of the VLAN interface. If no name is set using the **nameif** command, or if there is no **interface vlan** command, the display shows a dash (-).

Table 30-4 show switch vlan Fields

Field	Description
Status	Shows the status, up or down, to receive and send traffic to and from the VLAN in the switch. At least one switch port in the VLAN needs to be in an up state for the VLAN state to be up.
Ports	Shows the switch ports assigned to each VLAN. If a switch port is listed for multiple VLANs, it is a trunk port. The above sample output shows Ethernet 0/1 is a trunk port that carries VLAN 100 and 300.

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show vlan	Shows the VLANs for models that do not have built-in switches.
switchport mode	Sets the mode of the switch port to access or trunk mode.

show tcpstat

To display the status of the security appliance TCP stack and the TCP connections that are terminated on the security appliance (for debugging), use the **show tcpstat** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show tcpstat

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the security appliance. The TCP statistics displayed are described in Table 28.

Table 30-5 TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.

Table 30-5 TCP Statistics in the show tcpstat Command (continued)

Statistic	Description
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.
st	State (see RFC 793) of the TCP user. The possible values are as follows: 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack on the security appliance:

```
hostname# show tcpstat
                CURRENT MAX      TOTAL
tcb_cnt         2       12       320
proxy_cnt       0       0        160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
```

```
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

Command	Description
show conn	Displays the connections used and those that are available.

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**detail** | **file** | **no-config**]

Syntax Description

detail	(Optional) Lists detailed information.
file	(Optional) Writes the output of the command to a file.
no-config	(Optional) Excludes the output of the running configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	The **detail** and **file** keywords were added.
7.2(1)	The output display was enhanced to display more detailed information about processes that hog the CPU.

Usage Guidelines

The **show tech-suppor**t command lets you list information that technical support analysts need to help you diagnose problems. This command combines the output from the **show** commands that provide the most information to a technical support analyst.

Examples

The following example shows how to display information that is used for technical support analysis, excluding the output of the running configuration:

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
```

```
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Apr 17 2005

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
```

```
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show cpu hogging process ------------------

Process:      fover_parse, NUMHOG: 2, MAXHOG: 280, LASTHOG: 140
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           11a4d5
Traceback:    12135e  121893  121822  a10d8b  9fd061  114de6 113e56f
              777135  7a3858  7a3f59  700b7f  701fbf  14b984

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 XXX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 XXX/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 XXX/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 XXX/intf0
```

```
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 XXX/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 XXX/intf2
H*  0011d7f7 0009ff2c 0053e5b0        780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
```

```
URL Access              0/s             0/s
URL Server Req          0/s             0/s
TCP Fixup               0/s             0/s
TCPIntercept            0/s             0/s
HTTP Fixup              0/s             0/s
FTP Fixup               0/s             0/s
AAA Authen              0/s             0/s
AAA Author              0/s             0/s
AAA Account             0/s             0/s
```

Related Commands

Command	Description
show clock	Displays the clock for use with the Syslog Server (PFSS) and the Public Key Infrastructure (PKI) protocol.
show conn count	Displays the connections used and available.
show cpu	Display the CPU utilization information.
show failover	Displays the status of a connection and which security appliance is active
show memory	Displays a summary of the maximum physical memory and current free memory that is available to the operating system.
show perfmon	Displays information about the performance of the security appliance
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the security appliance.
show xlate	Displays information about the translation slot.

show threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can view statistics using the **show threat-detection rate** command in privileged EXEC mode.

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

Syntax Description

acl-drop	(Optional) Shows the rate for dropped packets caused by denial by access lists.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
bad-packet-drop	(Optional) Shows the rate for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
conn-limit-drop	(Optional) Shows the rate for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	(Optional) Shows the rate for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	(Optional) Shows the rate for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop**, **inspect-drop**, and **scanning-threat**.
icmp-drop	(Optional) Shows the rate for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	(Optional) Shows the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	(Optional) Shows the rate limit for dropped packets caused by an interface overload.
scanning-threat	(Optional) Shows the rate for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	(Optional) Shows the rate for dropped packets caused by an incomplete session, such as TCP SYN attack or no data UDP session attack.

Defaults

If you do not specify an event type, all events are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	Multiple System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded
- The total number of events over the fixed time periods.

The security appliance computes the event counts 60 times over the average rate interval; in other words, the security appliance checks the rate at the end of each burst period, for a total of 60 completed burst intervals. The unfinshed burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 10 minutes, then the burst interval is 10 seconds. If the last burst interval was from 3:00:00 to 3:00:10, and you use the **show** command at 3:00:15, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection rate** command:

```
hostname# show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
  10-min Interface:                0               0       0                  204
  1-hour Interface:               88               0       0               318225
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command, then view the hosts that are categorized as attackers and targets using the **show threat-detection scanning-threat** command in privileged EXEC mode.

show threat-detection scanning-threat [**attacker** | **target**]

Syntax Description

attacker	(Optional) Shows attacking host IP addresses.
target	(Optional) Shows targetted host IP addresses.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The display was modified to include “& Subnet List” in the heading text.

Examples

The following is sample output from the **show threat-detection scanning-threat** command:

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0
    192.168.1.249
   Latest Attacker Host & Subnet List:
    192.168.10.234
    192.168.10.0
    192.168.10.2
    192.168.10.3
    192.168.10.4
    192.168.10.5
    192.168.10.6
    192.168.10.7
    192.168.10.8
    192.168.10.9
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection shun	Shows the currently shunned hosts.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command, and you automatically shun attacking hosts, then view the currently shunned hosts using the **show threat-detection shun** command in privileged EXEC mode.

show threat-detection shun

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following is sample output from the **show threat-detection shun** command:

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection statistics host

After you enable threat statistics with the **threat-detection statistics host** command, view host statistics using the **show threat-detection statistics host** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Shows statistics for a particular host.
mask	(Optional) Sets the subnet mask for the host IP address.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The security appliance computes the event counts 60 times over the average rate interval; in other words, the security appliance checks the rate at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics host** command:

```
hostname# show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0              10580308
  8-hour Sent byte:                367               0       0              10580308
 24-hour Sent byte:                122               0       0              10580308
  1-hour Sent pkts:                 28               0       0                104043
  8-hour Sent pkts:                  3               0       0                104043
 24-hour Sent pkts:                  1               0       0                104043
  20-min Sent drop:                  9               0       1                 10851
  1-hour Sent drop:                  3               0       1                 10851
  1-hour Recv byte:               2697               0       0               9712670
  8-hour Recv byte:                337               0       0               9712670
 24-hour Recv byte:                112               0       0               9712670
  1-hour Recv pkts:                 29               0       0                104846
  8-hour Recv pkts:                  3               0       0                104846
 24-hour Recv pkts:                  1               0       0                104846
  20-min Recv drop:                 42               0       3                 50567
  1-hour Recv drop:                 14               0       1                 50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                   614
  8-hour Sent byte:                  0               0       0                   614
 24-hour Sent byte:                  0               0       0                   614
  1-hour Sent pkts:                  0               0       0                     6
  8-hour Sent pkts:                  0               0       0                     6
 24-hour Sent pkts:                  0               0       0                     6
  20-min Sent drop:                  0               0       0                     4
  1-hour Sent drop:                  0               0       0                     4
  1-hour Recv byte:                  0               0       0                   706
  8-hour Recv byte:                  0               0       0                   706
 24-hour Recv byte:                  0               0       0                   706
  1-hour Recv pkts:                  0               0       0                     7
```

Table 30-6 shows each field description.

Table 30-6 show threat-detection statistics host Fields

Field	Description
Host	Shows the host IP address.
tot-ses	Shows the total number of sessions for this host since it was added to the database.
act-ses	Shows the total number of active sessions that the host is currently involved in.

Table 30-6 show threat-detection statistics host Fields (continued)

Field	Description
fw-drop	Shows the number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including access list denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and no data UDP attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.
insp-drop	Shows the number of packets dropped because they failed application inspection.
null-ses	Shows the number of null sessions, which are TCP SYN sessions that did not complete within the 30-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.
bad-acc	Shows the number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see above), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 60 completed burst intervals. The unfinshed burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinshed burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Table 30-6 show threat-detection statistics host Fields (continued)

Field	Description
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the host.
Sent pkts	Shows the number of successful packets sent from the host.
Sent drop	Shows the number of packets sent from the host that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the host.
Recv pkts	Shows the number of successful packets received by the host.
Recv drop	Shows the number of packets received by the host that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics port

After you enable threat statistics with the **threat-detection statistics port** command, view TCP and UDP port statistics using the **show threat-detection statistics port** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **port** [*start_port*[*-end_port*]]

Syntax Description

start_port[*-end_port*]	(Optional) Shows statistics for a particular port or range of ports, between 0 and 65535.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The security appliance computes the event counts 60 times over the average rate interval; in other words, the security appliance checks the rate at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics port** command:

```
hostname# show threat-detection statistics port

                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

Table 30-6 shows each field description.

Table 30-7 show threat-detection statistics port Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00

Table 30-7 show threat-detection statistics port Fields (continued)

Field	Description
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
port_number/*port_name*	Shows the port number and name where the packet or byte was sent, received, or droppped.
tot-ses	Shows the total number of sessions for this port.
act-ses	Shows the total number of active sessions that the port is currently involved in.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the port.
Sent pkts	Shows the number of successful packets sent from the port.
Sent drop	Shows the number of packets sent from the port that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the port.
Recv pkts	Shows the number of successful packets received by the port.
Recv drop	Shows the number of packets received by the port that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics protocol

After you enable threat statistics with the **threat-detection statistics protocol** command, view IP protocol statistics using the **show threat-detection statistics protocol** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

Syntax Description

protocol_number	(Optional) Shows statistics for a specific protocol number, between 0 and 255.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
protocol_name	(Optional) Shows statistics for a specific protocol name: • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The security appliance computes the event counts 60 times over the average rate interval; in other words, the security appliance checks the rate at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics protocol** command:

```
hostname# show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

Table 30-6 shows each field description.

Table 30-8 show threat-detection statistics protocol Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
protocol_number/ *protocol_name*	Shows the protocol number and name where the packet or byte was sent, received, or droppped.
tot-ses	Shows the total number of sessions for this protocol.
act-ses	Shows the total number of active sessions that the protocol is currently involved in.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the protocol.
Sent pkts	Shows the number of successful packets sent from the protocol.
Sent drop	Shows the number of packets sent from the protocol that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the protocol.

Table 30-8 show threat-detection statistics protocol Fields (continued)

Field	Description
Recv pkts	Shows the number of successful packets received by the protocol.
Recv drop	Shows the number of packets received by the protocol that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics host	Shows the host statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics top

After you enable threat statistics with the **threat-detection statistics** command, view the top 10 statistics using the **show threat-detection statistics top** command in privileged EXEC mode. If you did not enable the threat detection statistics for a particular type, then you cannot view those statistics with this command. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**]]

Syntax Description

access-list	(Optional) Shows the top 10 ACEs that that match packets, including both permit and deny ACEs. Permitted and denied traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
all	(Optional) For TCP Intercept, shows the history data of all the traced servers.
detail	(Optional) For TCP Intercept, shows history sampling data.
host	(Optional) Shows the top 10 host statistics for each fixed time period.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
port-protocol	(Optional) Shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.
rate-1	(Optional) Shows the statistics for the smallest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-1** keyword, the security appliance shows only the 1 hour time interval.
rate-2	(Optional) Shows the statistics for the middle fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-2** keyword, the security appliance shows only the 8 hour time interval.
rate-3	(Optional) Shows the statistics for the largest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-3** keyword, the security appliance shows only the 24 hour time interval.
tcp-intercept	Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack.

Defaults

If you do not specify an event type, all events are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The **tcp-intercept** keyword was added.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The security appliance computes the event counts 60 times over the average rate interval; in other words, the security appliance checks the rate at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics top access-list** command:

```
hostname# show threat-detection statistics top access-list

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]              173                0       0                623488
              200/2[1]               43                0       0                156786
              100/1[2]               43                0       0                156786
  8-hour ACL hits:
              100/3[0]               21             1298       0                623488
              200/2[1]                5              326       0                156786
              100/1[2]                5              326       0                156786
```

Table 30-6 shows each field description.

Table 30-9 show threat-detection statistics top access-list Fields

Field	Description
Top	Shows the ranking of the ACE within the time period, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ACEs might be listed.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 60 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/60th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00.
Trigger	This column is always 0, because there are no rate limits triggered by access list traffic; denied and permitted traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 60) when calculating the total events. In that case, the security appliance calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
1-hour, 8-hour	Shows statistics for these fixed rate intervals.
acl_name/*line_number*	Shows the access list name and line number of the ACE that caused the denies.

The following is sample output from the **show threat-detection statistics top access-list rate-1** command:

```
hostname# show threat-detection statistics top access-list rate-1

                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]              173                0       0               623488
              200/2[1]               43                0       0               156786
```

```
              100/1[2]              43                0       0               156786
```

The following is sample output from the **show threat-detection statistics top port-protocol** command:

```
hostname# show threat-detection statistics top port-protocol

Top          Name    Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
 3         gopher   69              65               0       0          24345678
 4    Protocol-96 * 96              63               0       0          22345678
 5      Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7     Port-8191-65535              55               0       0          12345678
 8           SMTP  366              34               0       0           3345678
 9         IPinIP *  4              30               0       0           2345678
10          EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

Table 30-10 shows each field description.

Table 30-10 show threat-detection statistics top port-protocol Fields

Field	Description
Top	Shows the ranking of the port or protocol within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ports/protocols might be listed.
Name	Shows the port/protocol name.
Id	Shows the port/protocol ID number. The asterisk (*) means the ID is an IP protocol number.
Average(eps)	See the description in Table 30-6.
Current(eps)	See the description in Table 30-6.
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	See the description in Table 30-6.
Time_interval Sent byte	Shows the number of successful bytes sent from the listed ports and protocols for each time period.

Table 30-10 show threat-detection statistics top port-protocol Fields (continued)

Field	Description
Time_interval Sent packet	Shows the number of successful packets sent from the listed ports and protocols for each time period.
Time_interval Sent drop	Shows the number of packets sent for each time period from the listed ports and protocols that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed ports and protocols for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
port_number/*port_name*	Shows the port number and name where the packet or byte was sent, received, or droppped.
protocol_number/ *protocol_name*	Shows the protocol number and name where the packet or byte was sent, received, or droppped.

The following is sample output from the **show threat-detection statistics top host** command:

```
hostname# show threat-detection statistics top host

                  Top     Average(eps)     Current(eps) Trigger          Total events
  1-hour Sent byte:
         10.0.0.1[0]             2938                0       0              10580308
  1-hour Sent pkts:
         10.0.0.1[0]               28                0       0                104043
  20-min Sent drop:
         10.0.0.1[0]                9                0       1                 10851
  1-hour Recv byte:
         10.0.0.1[0]             2697                0       0              9712670
  1-hour Recv pkts:
         10.0.0.1[0]               29                0       0                104846
  20-min Recv drop:
         10.0.0.1[0]               42                0       3                 50567
  8-hour Sent byte:
         10.0.0.1[0]              367                0       0              10580308
  8-hour Sent pkts:
         10.0.0.1[0]                3                0       0                104043
  1-hour Sent drop:
         10.0.0.1[0]                3                0       1                 10851
  8-hour Recv byte:
         10.0.0.1[0]              337                0       0              9712670
  8-hour Recv pkts:
         10.0.0.1[0]                3                0       0                104846
  1-hour Recv drop:
         10.0.0.1[0]               14                0       1                 50567
 24-hour Sent byte:
         10.0.0.1[0]              122                0       0              10580308
 24-hour Sent pkts:
         10.0.0.1[0]                1                0       0                104043
 24-hour Recv byte:
         10.0.0.1[0]              112                0       0              9712670
 24-hour Recv pkts:
         10.0.0.1[0]                1                0       0                104846
```

Table 30-11 shows each field description.

Table 30-11 show threat-detection statistics top host Fields

Field	Description
Top	Shows the ranking of the host within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 hosts might be listed.
Average(eps)	See the description in Table 30-6.
Current(eps)	See the description in Table 30-6.
Trigger	See the description in Table 30-6.
Total events	See the description in Table 30-6.
Time_interval Sent byte	Shows the number of successful bytes sent to the listed hosts for each time period.
Time_interval Sent packet	Shows the number of successful packets sent to the listed hosts for each time period.
Time_interval Sent drop	Shows the number of packets sent for each time period to the listed hosts that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed hosts for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
host_ip_address	Shows the host IP address where the packet or byte was sent, received, or droppped.

The following is sample output from the **show threat-detection statistics top tcp-intercept** command:

```
hostname# show threat-detection statistics top tcp-intercept

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Table 30-12 shows each field description.

Table 30-12 show threat-detection statistics top tcp-intercept Fields

Field	Description
Monitoring window size:	Shows the period of time over which the security appliance samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The security appliance samples data 60 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 60.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the inerface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the sampling period
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip	Shows the attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.

The following is sample output from the **show threat-detection statistics top tcp-intercept detail** command:

```
hostname# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1     192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
      Sampling History (60 Samplings):
              95348      95337      95341      95339      95338      95342
              95337      95348      95342      95338      95339      95340
              95339      95337      95342      95348      95338      95342
              95337      95339      95340      95339      95347      95343
              95337      95338      95342      95338      95337      95342
              95348      95338      95342      95338      95337      95343
              95337      95349      95341      95338      95337      95342
              95338      95339      95338      95350      95339      95570
              96351      96351      96119      95337      95349      95341
              95338      95337      95342      95338      95338      95342
......
```

Table 30-13 shows each field description.

Table 30-13 show threat-detection statistics top tcp-intercept detail Fields

Field	Description
Monitoring window size:	Shows the period of time over which the security appliance samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The security appliance samples data 60 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 60.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the inerface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the rate interval set by the **threat-detection statistics tcp-intercept rate-interval** command (by default, the rate interval is 30 minutes). The security appliance samples the data every 30 seconds over the rate interval.
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip or <various> Last: *attacker_ip*	Shows the attacker IP address. If there is more than one attacker, then "<various>" displays followed by the last attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.
sampling data	Shows all 60 sampling data values, which show the number of attacks at each inerval.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show tls-proxy

To display TLS proxy and session information, use the **show tls-proxy** command in global configuration mode.

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**]]

Syntax Description

cert-dump	Dumps the local dynamic certificate. Output is a hex dump of the LDC.
count	Shows only the session counters.
detail	Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC.
host *host_addr*	Specifies a particular host to show the sessions associated with.
session	Shows active TLS proxy sessions.
tls_name	Name of the TLS proxy to show.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC mode	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following is sample output from the **show tls-proxy** command:

```
hostname# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
    Server proxy:
        Trust-point: local_ccm
    Client proxy:
        Local dynamic certificate issuer: ldc_signer
        Local dynamic certificate key-pair: phone_common
        Cipher-suite <unconfigured>
    Run-time proxies:
        Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
            Active sess 1, most sess 4, byte 3244
```

The following is sample output from the **show tls-proxy session** command:

```
hostname# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
```

```
S:0x482e790 byte 3388
```

The following is sample output from the **show tls-proxy session detail** command:

```
hostname# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
    Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
    Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
    Status: Available
    Certificate Serial Number: 29
    Certificate Usage: General Purpose
    Public Key Type: RSA (1024 bits)
    Issuer Name:
        cn=TLS-Proxy-Signer
    Subject Name:
        cn=SEP0002B9EB0AAD
        o=Cisco Systems Inc
        c=US
    Validity Date:
        start date: 00:47:12 PDT Feb 27 2007
        end   date: 00:47:12 PDT Feb 27 2008
    Associated Trustpoints:
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show running-config tls-proxy	Shows running configuration of all or specified TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show track

To display information about object tracked by the tracking process, use the **show track** command in user EXEC mode.

show track [*track-id*]

Syntax Description

track-id	A tracking entry object ID. Valid values are from 1 to 500.

Defaults

If the *track-id* is not provided, then information about all tracking objects is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show track** command:

```
hostname(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

Related Commands

Command	Description
show running-config track	Displays the **track rtr** commands in the running configuration.
track rtr	Creates a tracking entry to poll the SLA.

show traffic

To display interface transmit and receive activity, use the **show traffic** command in privileged EXEC mode.

show traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	Special display for the ASA 5550 adaptive security appliance was added.

Usage Guidelines

The **show traffic** command lists the number of packets and bytes moving through through each interface since the last show traffic command was entered or since the security appliance came online. The number of seconds is the duration the security appliance has been online since the last reboot, unless the **clear traffic** command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

For the ASA 5550 adaptive security appliance, the **show traffic** command also shows the aggregated throughput per slot. Because the ASA 5550 adaptive security appliance requires traffic to be evenly distributed across slots fro maximum throughput, this display helps you determine if the traffic is distributed evenly.

Examples

The following example shows output from the **show traffic** command:

```
hostname# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
```

```
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

For the ASA 5550 adaptive security appliance, the following text is displayed at the end:

```
----------------------------------------
        Per Slot Throughput Profile
----------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************

  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

Related Commands

Command	Description
clear traffic	Resets the counters for transmit and receive activity.

show uauth

To display one or all currently authenticated users, the host IP to which they are bound, and any cached IP and port authorization information, use the **show uauth** command in privileged EXEC mode.

show uauth [*username*]

Syntax Description

username	(Optional) Specifies, by username, the user authentication and authorization information to display.

Defaults

Omitting username displays the authorization information for all users.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show uauth** command displays the AAA authorization and authentication caches for one user or for all users.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. The cache allows up to 16 address and service pairs for each user host. If the user attempts to access a service that has been cached from the correct host, the security appliance considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is authenticated only or has cached services.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry

cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see to the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows sample output from the **show uauth** command when no users are authenticated and one user authentication is in progress:

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the security appliance:

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

Related Commands

Command	Description
clear uauth	Remove current user authentication and authorization information.
timeout	Set the maximum idle time duration.

show url-block

To display the number of packets held in the url-block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission, use the **show url-block** command in privileged EXEC mode.

show url-block [**block statistics**]

Syntax Description

block statistics	(Optional) Displays block buffer usage statistics.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show url-block block statistics** command displays the number of packets held in the url block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission.

Examples

The following is sample output from the **show url-block** command:

```
hostname# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

This shows the configuration of the URL block buffer.

The following is sample output from the **show url-block block statistics** command:

```
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show url-cache statistics

To display information about the url-cache, which is used for URL responses received from an N2H2 or Websense filtering server, use the **show url-cache statistics** command in privileged EXEC mode.

show url-cache statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show url-cache statistics** command displays the following entries:

- Size—The size of the cache in kilobytes, set with the **url-cache** *size* option.
- Entries—The maximum number of cache entries based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times the security appliance has looked for a cache entry.
- Hits—The number of times the security appliance has found an entry in the cache.

You can view additional information about N2H2 Sentian or Websense filtering activity with the **show perfmon** command.

Examples

The following is sample output from the **show url-cache statistics** command:

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 Hits :     290
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching for responses received from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show url-server

To display information about the URL filtering server, use the **show url-server** command in privileged EXEC mode.

show url-server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show url-server statistics** command displays the URL server vendor; number of URLs total, allowed, and denied; number of HTTPS connections total, allowed, and denied; number of TCP connections total, allowed, and denied; and the URL server status.

The **show url-server** command displays the following information:

- For N2H2, **url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- For Websense, **url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

Examples

The following is sample output from the **show url-server statistics** command:

```
hostname## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
```

```
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                       DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                  Sent     Received
STATUS_REQUEST           411      0
LOOKUP_REQUEST           366519   365952
LOG_REQUEST              0        NA

Errors:
-------
RFC noncompliant GET method       0
URL buffer update failure         0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis.  The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show version

To display the software version, hardware configuration, license key, and related uptime data, use the **show version** command in user EXEC mode.

show version

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	In stateful failover mode, an additional line showing cluster uptime is displayed.

Usage Guidelines

The **show version** command allows you to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type (R or UR), and time stamp for when the configuration was last modified.

The serial number listed with the **show version** command is for the Flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the **show version** command, not the chassis number.

- If you downgrade to an earlier release, your key for the current release might allow for more security contexts than the earlier release supports. When the value of the security contexts in the key exceeds the platform limit, the following message appears in the show activation-key output:

  ```
  The Running Activation Key feature: 50 security contexts exceeds the limit in the
  platform, reduce to 20 security contexts.
  ```

- If you downgrade to an earlier release, your key for the current release might enable GTP/GPRS even though it is not allowed in the earlier release. When the key enables GTP/GPRS but the software version does not allow it, the following message appears in the show activation-key output:

  ```
  The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
  GTP/GPRS.
  ```

The failover cluster uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value continues to increase as long as the active unit continues to operate. Therefore, it is possible for the failover cluster uptime to be greater than the individual unit uptime. If you temporarily disable failover, and then reenable it, the failover cluster uptime reports the time the unit was up before failover was disabled plus the time the unit was up while failover was disabled.

Examples

The following example shows how to display the software version, hardware configuration, license key, and related uptime information. Note that in an environment where stateful failover is configured an additional line showing the failover cluster uptime is displayed. If failover is not configured, the line is not displayed:

```
hostname# show version

Cisco Adaptive Security Appliance Software Version 8.0(0)
Device Manager Version 6.0(0)

Compiled on Mon 16-April-07 03:29 by root
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/main_backup.cfg"

hostname up 2 days 10 hours
failover cluster up 2 days 11 hours

Hardware:   ASA5520, 1024 MB RAM, CPU Pentium 4 Celeron 2000 MHz
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.01
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.04
 0: Ext: GigabitEthernet0/0  : address is 000b.fcf8.c44e, irq 9
 1: Ext: GigabitEthernet0/1  : address is 000b.fcf8.c44f, irq 9
 2: Ext: GigabitEthernet0/2  : address is 000b.fcf8.c450, irq 9
 3: Ext: GigabitEthernet0/3  : address is 000b.fcf8.c451, irq 9
 4: Ext: Management0/0       : address is 000b.fcf8.c44d, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 150
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 10
GTP/GPRS                     : Enabled
VPN Peers                    : 750
WebVPN Peers                 : 500
Advanced Endpoint Assessment : Disabled

This platform has an ASA 5520 VPN Plus license.

Serial Number: P3000000098
Running Activation Key: 0x7c2e394b 0x0c842e53 0x98f3edf0 0x8c1888b0 0x0336f1ac
Configuration register is 0x1
Configuration last modified by enable_15 at 14:17:59.410 EST Wed April 16 2007
hostname#
```

The following message appears if you enter the **show version** command after the **eject** command has been executed, but the device has not been physically removed:

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

Related Commands

Command	Description
eject	Allows shutdown of external compact Flash device before physical removal from the security appliance.
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the security appliance has been up.

show vlan

To display all VLANs configured on the security appliance, use the **show vlan** command in privileged EXEC mode.

show vlan

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays the configured VLANs:

```
hostname# show vlan
10-11, 30, 40, 300
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show vpn load-balancing

To display the runtime statistics for the VPN load-balancing virtual cluster configuration, use the **show vpn-load-balancing** command in global configuration, privileged EXEC, or VPN load-balancing mode.

show vpn load-balancing

Syntax Description

This command has no variables or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added separate IPSec and SSL columns for both Load (%) display and Session display in the output example.

Usage Guidelines

The **show vpn load-balancing** command displays statistical information for the virtual VPN load-balancing cluster. If the local device is not participating in the VPN load-balancing cluster, this command indicates that VPN load balancing has not been configured for this device.

The load balancing cluster master receives a periodic message from each ASA in the cluster with the number of active AnyConnect and clientless sessions, as well as the maximum allowed sessions based on the configured or license limits. If an ASA in the cluster shows 100% full capacity, the cluster master cannot redirect more connections to it. Although the ASA may show as full, some users may be in Inactive/wait-to-resume state, wasting the licenses. As a workaround, each ASA provides the total number of sessions minus the sessions in inactive state, instead of the total number of sessions. In other words, the inactive sessions are not reported to the cluster master. Even if the ASA is full (with some inactive sessions), the cluster master still redirects connections to it if necessary. When the ASA receives the new connection, the session that has been inactive the longest is logged off, allowing new connections to take its license.

The asterisk (*) in the output indicates the IP address of the security appliance to which you are connected.

Examples

This example displays **show vpn load-balancing** command and its output for a situation in which the local device is participating in the VPN load-balancing cluster:

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
                                              Load (%)           Sessions
Public IP       Role   Pri     Model          IPSec  SSL        IPSec   SSL
------------------------------------------------------------------------------
* 192.168.1.40  Master 10     PIX-515         0       0          0       0
  192.168.1.110  Backup   5 PIX-515          0       0          0       0
hostname(config-load-balancing)#
```

Note Sessions that are inactive are sorted from the longest time to the shortest time. Inactive SSL sessions are not counted and do not appear in the sessions and load totals.

If the local device is not participating in the VPN load-balancing cluster, the **show vpn load-balancing** command shows a different result:

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
vpn load-balancing	Enters vpn load-balancing mode.

show vpn-sessiondb

To display information about VPN sessions, use the show **vpn-sessiondb** command in privileged EXEC mode. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information. The syntax table and usage notes organize the choices accordingly.

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* | **webvpn | email-proxy | svc} [filter {name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo* | **inactive***}***] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption | inactivity}]**

Syntax Descriptions

Granularity of Display	Description
detail	Displays extended details about a session. For example, using the **detail** option for an IPSec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval. If you choose **detail**, and the **full** option, the security appliance displays the detailed output in a machine-readable format.
filter *filter_criteria*	(Optional) Filters the output to display only the information you specify by using one or more of the filter options. For more information, see usage notes.
full	Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.
sort	Sorts the output according to the sort option you specify. For more information, see usage notes.
Session Type to Display	**Description**
email-proxy	Displays email-proxy sessions. You can display this information for e-mail proxy sessions, or you can filter it by using the following filter and sort options: **name** (connection name), **ipaddress** (client), **encryption**.
index *indexnumber*	Displays a single session by index number. Specify the index number for the session, 1 - 750. Filter and sort options do not apply.
l2l	Displays VPN LAN-to-LAN session information. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **protocol, encryption**.
remote	Displays remote-access sessions. You can display this information for all groups or you can filter it by using the following filter options: **name**, **a-ipaddress**, **p-ipaddress, tunnel-group**, **protocol**, **encryption**.
webvpn	Displays information about WebVPN sessions. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **encryption**.
svc	Configures SSL VPN client attributes.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.3(0)	Added VLAN field description.
7.2(1)	This command was introduced.
8.0(5)	Added **inactive** as a **filter** option and **inactivity** as a **sort** option.

Usage Guidelines

You can use the following options to filter and to sort the session display:

Filter/Sort Option	Description
filter a-ipaddress *IPaddr*	Filters the output to display information for the specified assigned IP address or addresses only.
sort a-ipaddress	Sorts the display by assigned IP addresses.
filter encryption *encryption-algo*	Filters the output to display information for sessions using the specified encryption algorithm(s) only.
sort encryption	Sorts the display by encryption algorithm. Encryption algorithms include: aes128, aes192, aes256, des, 3des, rc4
filter inactive	Filters inactive sessions which have lost connectivity. Each session is time stamped with the SSL tunnel drop time. If the session is active, 00:00m:00s is displayed.
sort inactivity	Sorts inactive sessions.
filter ipaddress *IPaddr*	Filters the output to display information for the specified inside IP address or addresses only.
sort ipaddress	Sorts the display by inside IP addresses.
filter name *username*	Filters the output to display sessions for the specified username(s).
sort name	Sorts the display by usernames in alphabetical order.
filter p-address *IPaddr*	Filters the output to display information for the specified outside IP address only.
sort p-address	Sorts the display by the specified outside IP address or addresses.
filter protocol *protocol-name*	Filters the output to display information for sessions using the specified protocol(s) only.
sort protocol	Sorts the display by protocol. Protocols include: IKE, IMAP4S, IPSec, IPSecLAN2LAN, IPSecLAN2LANOverNatT, IPSecOverNatT, IPSecoverTCP, IPSecOverUDP, SMTPS, userHTTPS, vcaLAN2LAN
filter tunnel-group *groupname*	Filters the output to display information for the specified tunnel group(s) only.

Filter/Sort Option	Description
sort tunnel-group	Sorts the display by tunnel group.
| character	Modifies the output, using the following arguments: {begin | include | exclude | grep | [-v]} {reg_exp}
<cr>	Sends the output to the console.

The following example, entered in privileged EXEC mode, shows detailed information about LAN-to-LAN sessions:

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.1
Index        : 1                     IP Addr      : 172.16.0.1
Protocol     : IPSecLAN2LAN          Encryption   : AES256
Bytes Tx     : 48484156              Bytes Rx     : 875049248
Login Time   : 09:32:03 est Mon Aug 2 2004
Duration     : 6:16:26
Filter Name  :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 63814 Seconds
  D/H Group    : 5

IPSec:
  Session ID   : 2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224              Bytes Rx     : 2639672
  Pkts Tx      : 1635314               Pkts Rx      : 37526


IPSec:
  Session ID   : 3
  Local Addr   : 10.0.0.1/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 6282 Seconds
  Bytes Tx     : 1619268               Bytes Rx     : 872409912
  Pkts Tx      : 19277                 Pkts Rx      : 1596809

hostname#
```

The following example shows the details of single session:

```
AsaNacDev# show vpn-sessiondb detail full index 4
Session Type: Remote Detailed |
```

```
Index: 2 | EasyVPN: 0 | Username: uuuu | Group: DfltGrpPolicy | Tunnel Group:
regr3000multigroup | IP Addr: 192.168.2.80 | Public IP: 161.44.173.216 | Protocol:
IPSecOverUDP | Encryption: 3DES | Login Time: 12:51:54 EDT Wed Jun 21 2006 |Duration:
0h:02m:44s | Bytes Tx: 2134 | Bytes Rx: 8535 | Client Type: WinNT | Client Ver: 4.0.5
(Rel) | Filter Name:  | NAC Result: N/A | Posture Token: : | VM Result: Static | VLAN: 10
||

IKE Sessions: 1
 | IPSecOverUDP Sessions: 1
 |

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeys | UDP Source Port: 500 |
UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES | Hashing:
SHA1 | Diffie-Hellman Group: 2 | Rekey Time Interval: 40000 Seconds| Rekey Left(T): 39836
Seconds ||

Type: IPSecOverUDP | Session ID: 2 | Local IP Addr: 0.0.0.0/0.0.0.0/0/0 | Remote IP Addr:
192.168.2.80/255.255.255.255/0/0 | Encryption: 3DES | Hashing: SHA1 | Encapsulation:
Tunnel | UDP Destination Port: 10000 | Rekey Time Interval: 28800 Seconds | Rekey Left(T):
28636 Seconds | Idle Time Out: 30 Minutes | Idle TO Left: 30 Minutes | Bytes Tx: 2134 |
Bytes Rx: 8535 | Packets Tx: 15 | Packets Rx: 2134 | ||

VLAN Mapping: VLAN: 10 |

AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : dbrownhi
Index        : 1
Assigned IP  : 192.168.2.70          Public IP    : 10.86.5.114
Protocol     : IPSec                 Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                     Bytes Rx     : 604533
Client Type  : WinNT                 Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10

IKE Sessions: 1 IPSec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                     Bytes Rx     : 604533
  Pkts Tx      : 0                     Pkts Rx      : 8126
```

```
NAC:
  Reval Int (T): 3000 Seconds           Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds            EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds              Posture Token: Healthy
  Redirect URL : www.cisco.com
```

As shown in the examples, the fields displayed in response to the **show vpn-sessiondb** command vary, depending on the keywords you enter. Table 30-14 explains these fields.

Table 30-14 show vpn-sessiondb Command Fields

Field	Description
Auth Mode	Protocol or mode used to authenticate this session.
Bytes Rx	Total number of bytes received from the remote peer or client by the security appliance.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the security appliance.
Client Type	Client software running on the remote peer, if available.
Client Ver	Version of the client software running on the remote peer.
Connection	Name of the connection or the private IP address.
D/H Group	Diffie-Hellman Group. The algorithm and key size used to generate IPSec SA encryption keys.
Duration	Elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
EAPoUDP Session Age	Number of seconds since the last successful posture validation.
Encapsulation	Mode used to apply IPSec ESP (Encapsulation Security Payload protocol) encryption and authentication (that is, the part of the original IP packet that has ESP applied).
Encryption	Data encryption algorithm this session is using, if any.
Encryption	Data encryption algorithm this session is using.
EoU Age (T)	EAPoUDP Session Age. Number of seconds since the last successful posture validation.
Filter Name	Username specified to restrict the display of session information.
Hashing	Algorithm used to create a hash of the packet, which is used for IPSec data authentication.
Hold Left (T)	Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
Hold-Off Time Remaining	0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
IKE Neg Mode	IKE (IPSec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	Number of IKE (IPSec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPSec traffic.
Index	Unique identifier for this record.

Table 30-14 show vpn-sessiondb Command Fields

Field	Description
IP Addr	Private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address. It lets the client appear to be a host on the private network.
IPSec Sessions	Number of IPSec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPSec remote-access session can have two IPSec sessions: one consisting of the tunnel endpoints, and one consisting of the private networks reachable through the tunnel.
Local IP Addr	IP address assigned to the local endpoint of the tunnel (that is the interface on the security appliance).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
NAC Result	State of Network Admission Control Posture Validation. It can be one of the following: • Accepted—The ACS successfully validated the posture of the remote host. • Rejected—The ACS could not successfully validate the posture of the remote host. • Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the security appliance. • Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. • Hold-off—The security appliance lost EAPoUDP communication with the remote host after successful posture validation. • N/A—NAC is disabled for the remote host according to the VPN NAC group policy. • Unknown—Posture validation is in progress.
NAC Sessions	Number of Network Admission Control (EAPoUDP) sessions.
Packets Rx	Number of packets received from the remote peer by the security appliance.
Packets Tx	Number of packets transmitted to the remote peer by the security appliance.
PFS Group	Perfect Forward Secrecy group number.
Posture Token	Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the security appliance for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
Protocol	Protocol the session is using.
Public IP	Publicly routable IP address assigned to the client.

Table 30-14 show vpn-sessiondb Command Fields

Field	Description
Redirect URL	Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the security appliance. The Redirect URL is an optional part of the access policy payload. The security appliance redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the security appliance does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPSec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.
Rekey Int (T)	Lifetime of the IPSec (IKE) SA encryption keys.
Rekey Left (T)	Lifetime remaining of the IPSec (IKE) SA encryption keys.
Rekey Time Interval	Lifetime of the IPSec (IKE) SA encryption keys.
Remote IP Addr	IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).
Reval Int (T)	Revalidation Time Interval. Interval in seconds required between each successful posture validation.
Reval Left (T)	Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Revalidation Time Interval	Interval in seconds required between each successful posture validation.
Session ID	Identifier for the session component (subsession). Each SA has its own identifier.
Session Type	Type of session: LAN-to-LAN or Remote
SQ Int (T)	Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the security appliance to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Status Query Time Interval	Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the security appliance to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Time Until Next Revalidation	0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Tunnel Group	Name of the tunnel group referenced by this tunnel for attribute values.
UDP Dst Port or UDP Destination Port	Port number used by the remote peer for UDP.

Table 30-14 show vpn-sessiondb Command Fields

Field	Description
UDP Src Port or UDP Source Port	Port number used by the security appliance for UDP.
Username	User login name with which the session is established.
VLAN	Egress VLAN interface assigned to this session. The security appliance forwards all traffic to that VLAN. One of the following elements specifies the value: • Group policy • Inherited group policy

Related Commands

Command	Description
show running-configuration vpn-sessiondb	Displays the VPN session database running configuration.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.
show vpn-sessiondb summary	Displays a summary of all VPN sessions.

show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the **show vpn-sessiondb ratio** command in privileged EXEC mode.

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

Syntax Description

encryption	Identifies the encryption protocols you want to display. Refers to phase 2 encryption. Encryption algorithms include: aes128 — des aes192 — 3des aes256 — rc4
filter *groupname*	Filters the output to include session ratios only for the tunnel group you specify.
protocol	Identifies the protocols you want to display. Protocols include: IKE — SMTPS IMAP4S — userHTTPS IPSec — vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

```
hostname# show vpn-sessiondb ratio enc
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

The following is sample output for the **show vpn-sessiondb ratio** command with **protocol** as the argument:

```
hostname# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPSec                    1              20%
IPSecLAN2LAN             0               0%
IPSecLAN2LANOverNatT     0               0%
IPSecOverNatT            0               0%
IPSecOverTCP             1 20%
IPSecOverUDP             0               0%
L2TP                     0               0%
L2TPOverIPSec            0               0%
L2TPOverIPSecOverNatT    0               0%
PPPoE                    0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

Related Commandss

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show vpn-sessiondb summary

To display the number of IPSec, Cisco AnyConnect, and NAC sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode.

show vpn-sessiondb summary

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	—	•

Command History

Release	Modification
7.3(0)	Added the VLAN Mapping Sessions table.
7.2(1)	This command was introduced.
8.0(5)	Added new output for active, cumulative, peak concurrent, and inactive.

Examples

The following is sample output for the **show vpn-sessiondb summary** command on an active device:

Note A device in standby does not differentiate active from inactive sessions.

```
hostname# show vpn-sessiondb summary

Active Session Summary
Sessions:
                  Active :Cumulative :Peak Concurrent :Inactive :
  SSL VPN  :          0 :         1 :               1 :
    Clientless only   0 :         1 :               1 :
    With client       0 :         0 :               0 :         0
Totals                0 :         1

License Information:
    Shared VPN License Information:
        SSL VPN                     : 12000
            Allocated to this device  :    0
            Allocated to network      :    0
            Device limit              : 750

IPsec   :   750     Configured :750    Active : 0     Load : 0%
SSL VPN :   750     Configured :750    Active : 0     Load : 0%
                        Active : Cumulative : Peak Concurrent
SSL VPN         :           0 :         1 :            1
Totals          :           0 :         1 :
```

```
Active NAC Sessions:
  Accepted               : 0
  Rejected               : 0
  Exempted               : 0
  Non-responsive         : 0
Hold-off               : 0
  N/A                    : 0

Active VLAN Mapping Sessions:
  Static                 : 0
  Auth                   : 0
  Access                 : 0
  Guest                  : 0
  Quarantine             : 0
  N/A                    : 0

F1-asa1#
```

A session is a VPN tunnel established with a specific peer. An IPSec LAN-to-LAN tunnel counts as one session, and it allows many host-to-host connections through the tunnel. An IPSec remote access session is one remote access tunnel that supports one user connection.

The Active SSL VPN With Client column shows the number of active connections passing data. The Cumulative SSL VPN With Client column shows the number of active sessions that have been established. It includes those that are inactive and increments only when a new session is added. The Peak Concurrent SSL VPN With Client column shows the peak number of concurrently active sessions that are passing data. The Inactive SSL VPN With Client column shows inactive sessions. These are AnyConnect sessions without an active SSL tunnel associated with them.

Table 30-15 explains the fields in the Active Sessions and Session Information tables.

Table 30-15 show vpn-sessiondb summary Command: Active Sessions and Session Information Fields

Field	Description
Concurrent Limit	Maximum number of concurrently active sessions permitted on this security appliance.
Cumulative Sessions	Number of sessions of all types since the security appliance was last booted or reset.
LAN-to-LAN	Number of IPSec LAN-to-LAN sessions that are currently active.
Peak Concurrent	Highest number of sessions of all types that were concurrently active since the security appliance was last booted or reset.
Percent Session Load	Percentage the vpn session allocation in use. This value equals the Total Active Sessions divided by the maximum number of sessions available, displayed as a percentage. The maximum number of sessions available can be either of the following: • Maximum number of IPSec and SSL VPN sessions licensed. • Maximum number of sessions configured using the following commands: – **vpn-sessiondb max-session-limit** – **vpn-sessiondb max-webvpn-session-limit**

Table 30-15 show vpn-sessiondb summary Command: Active Sessions and Session Information Fields

Field	Description
Remote Access	Number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.
Total Active Sessions	Number of sessions of all types that are currently active.

The Active NAC Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative NAC Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 30-14 explains the fields in the Active NAC Sessions and Total Cumulative NAC Sessions tables.

Table 30-16 show vpn-sessiondb summary Command: Active NAC Sessions and Total Cumulative NAC Sessions Fields

Field	Description
Accepted	Number of peers that passed posture validation and have been granted an access policy by an Access Control Server.
Exempted	Number of peers that are not subject to posture validation because they match an entry in the Posture Validation Exception list configured on the security appliance.
Hold-off	Number of peers for which the security appliance lost EAPoUDP communications after a successful posture validation. The NAC Hold Timer attribute (Configuration > VPN > NAC) determines the delay between this type of event and the next posture validation attempt for each peer.
N/A	Number of peers for which NAC is disabled according to the VPN NAC group policy.
Non-responsive	Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the security appliance configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the security appliance for these peers. Otherwise, the security appliance assigns the NAC default policy.
Rejected	Number of peers that failed posture validation or were not granted an access policy by an Access Control Server.

The Active VLAN Mapping Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative VLAN Mapping Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 30-17 explains the fields in the Active VLAN Mapping Sessions and Cumulative VLAN Mapping Sessions tables.

Table 30-17 show vpn-sessiondb summary Command: Active VLAN Mapping Sessions and Cumulative Active VLAN Mapping Sessions Fields

Field	Description
Access	Reserved for future use.
Auth	Reserved for future use.
Guest	Reserved for future use.
N/A	Reserved for future use.
Quarantine	Reserved for future use.
Static	This field shows the number of VPN sessions assigned to a pre-configured VLAN.

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the **show wccp** command in privileged EXEC mode.

show wccp {**web-cache** | *service-number*}[*detail* | *view*]

Syntax Description

web-cache	Specifies statistics for the web-cache service.
service-number	(Optional) Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 256. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.
detail	(Optional) Displays information about the router and all web caches.
view	(Optional) Displays other members of a particular service group have or have not been detected.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to display WCCP information:

```
hostname(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
```

```
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
hostname(config)#
```

Related Commands

Commands	Description
wccp	Enables support of WCCP with service groups.
wccp redirect	Enables support of WCCP redirection.

show webvpn csd

To determine whether CSD is enabled and, if so, display the CSD version in the running configuration, or test a file to see if it is a valid CSD distribution package, use the **show webvpn csd** command in privileged EXEC mode.

show webvpn csd [**image** *filename*]

Syntax Description

filename	Specifies the name of a file to test for validity as a CSD distribution package. It must take the form securedesktop_asa_<*n*>_<*n*>*.pkg.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
privileged EXEC mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use the **show webvpn csd** command to check the operational status of CSD. The CLI responds with one of the following messages when you enter this command:

- `Secure Desktop is not enabled.`

  CSD is in the running configuration, but it is disabled. Go to webvpn configuration mode and enter the **csd enable** command to enable CSD.

- `Secure Desktop version n.n.n.n is currently installed and enabled.`

  CSD is enabled. The distribution package read from the flash device determines the version number. You can access Cisco Secure Desktop Manager through the ASDM Configuration > CSD menu path. CSD is accessible to users only if the CSD configuration contains a location.

Use the **show webvpn csd image** command to test a file to see if it is a valid CSD distribution package. Similarly, the **csd image** command, when entered in webvpn configuration mode, installs CSD only if the file you name in the command is a valid CSD distribution package. Otherwise, it displays an "ERROR: Unable to use CSD image" message.

The **show webvpn csd image** command tests a file to see if it is a valid CSD distribution package without installing CSD automatically if the file is valid. The CLI responds with one of the following messages when you enter this command:

- `ERROR: This is not a valid Secure Desktop image file.`

  Make sure the filename is in the form the form securedesktop_asa_<*n*>_<n>*.pkg. If it is, replace the file with a fresh one obtained from the following website:

  http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

  Then reenter the **show webvpn csd image** command. If the image is valid, use the **csd image** and **csd enable** commands in webvpn configuration mode to install and enable CSD.

- This is a valid Cisco Secure Desktop image:
  Version : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

  Note that the CLI provides both the version and date stamp if the file is valid.

Examples

The following example indicates CSD is installed in the running configuration and enabled:

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname#
```

The following example shows the file specified is a valid CSD image:

```
hostname#show webvpn csd image securedesktop_asa_3_1_0_25.pkg

This is a valid Cisco Secure Desktop image:
  Version  : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

hostname#
```

Related Commands

Command	Description
csd enable	Enables CSD for management and remote user access.
csd image	Copies the CSD image named in the command, from the flash drive specified in the path to the running configuration.

show webvpn group-alias

To display the aliases for a specific tunnel-group or for all tunnel groups, use the **group-alias** command in privileged EXEC mode.

show webvpn group-alias [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the group aliases.

Defaults

If you do not enter a tunnel-group name, this command displays all the aliases for all the tunnel groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1	This command was introduced.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-alias** command.

Each tunnel group can have multiple aliases or no alias.

Examples

The following example shows the **show webvpn group-alias** command that displays the aliases for the tunnel group “devtest” and the output of that command:

```
hostname# show webvpn group-alias devtest
QA
Fra-QA
```

Related Commands

Command	Description
group-alias	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn group-url

To display the URLs for a specific tunnel-group or for all tunnel groups, use the **group-url** command in privileged EXEC mode.

show webvpn group-url [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the URLs.

Defaults

If you do not enter a tunnel-group name, this command displays all the URLs for all the tunnel groups.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-url** command. Each group can have multiple URLs or no URL.

Examples

The following example shows the **show webvpn group-url** command that displays the URLs for the tunnel group "frn-eng1" and the output of that command:

```
hostname# show webvpn group-url
http://www.cisco.com
https://fra1.vpn.com
https://fra2.vpn.com
```

Related Commands

Command	Description
group-url	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn sso-server

To display the operating statistics for Webvpn single sign-on servers, use the **show webvpn sso-server** command in privileged EXEC mode.

show webvpn sso-server [*name*]

Syntax Description

name	Optionally specifies the name of the SSO server. The server name must be between four and 31 characters in length.

Defaults

No default values or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **show webvpn sso-server** command displays operating statistics for any and all SSO servers configured on the security device.

If no SSO server name argument is entered, statistics for all SSO servers display.

Examples

The following example, entered in privileged EXEC mode, displays statistics for a SiteMinder-type SSO server named example:

```
hostname# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
```

```
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
hostname#
```

The following example of the command issued without a specific SSO server name, displays statistics for all configured SSO servers on the security appliance:

```
hostname#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
asa1(config-webvpn)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

show webvpn svc

To view information about SSL VPN client images installed on the security appliance and loaded in cache memory, or to test a file to see if it is a valid client image, use the **show webvpn svc** command from privileged EXEC mode.

show webvpn svc [**image** *filename*]

Syntax Description

image *filename*	Specifies the name of a file to test as an SSL VPN client image file.

Defaults

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use the **show webvpn svc** command to view information about SSL VPN client images that are loaded in cache memory and available for download to remote PCs. Use the **image** *filename* keyword and argument to test a file to see if it is a valid image. If the file is not a valid image, the following message appears:

```
ERROR: This is not a valid SSL VPN Client image file.
```

Examples

The following example shows the output of the **show webvpn svc** command for currently installed images:

```
hostname# show webvpn svc
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

The following example shows the output of the **show webvpn svc image** *filename* command for a valid image:

```
F1(config-webvpn)# show webvpn svc image sslclient-win-1.0.2.127.pkg

This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

Related Commands

Command	Description
svc enable	Enables the security appliance to download the SSL VPN client to remote PCs.
svc image	Causes the security appliance to load SSL VPN client files from flash memory to cache memory, and specifies the order in which the security appliance downloads portions of the client image to the remote PC as it attempts to match the client image with the operating system.
vpn-tunnel-protocol	Enables specific VPN tunnel protocols for remote VPN users, including SSL used by an SSL VPN client.

show xlate

To display information about the translation slots, use the **show xlate** command in privileged EXEC mode.

show xlate [**global** *ip1*[*-ip2*] [**netmask** *mask*]] [**local** *ip1*[*-ip2*] [**netmask** *mask*]] [**gport** *port1*[*-port2*]] [**lport** *port1*[*-port2*]] [**interface** *if_name*] [**state** *state*] [**debug**] [**detail**]

show xlate count

Syntax Description

count	Displays the translation count.
debug	(Optional) Displays xlate debug information.
detail	(Optional) Displays detail xlate information.
global *ip1*[*-ip2*]	(Optional) Displays the active translations by global IP address or range of addresses.
gport *port1*[*-port2*]	Displays the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1*[*-ip2*]	(Optional) Displays the active translations by local IP address or range of addresses.
lport *port1*[*-port2*]	Displays the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Displays the active translations by state. You can enter one or more of the following states: • **static**—specifies **static** translations. • **portmap**—specifies PAT global translations. • **norandomseq**—specifies a **nat** or **static** translation with the **norondomseq** setting. • **identity**—specifies **nat 0** identity address translations. When specifying more than one state, separate the states with a space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show xlate** command displays the contents of the translation slots. The **show xlate detail** command displays the following information:

- {**ICMP**|**TCP**|**UDP**} **PAT from** *interface*:*real-address*/*real-port* **to** *interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*
- **NAT from** *interface*:*real-address*/*real-port to interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*

The translation flags are defined in Table 30-18.

Table 30-18 Translation Flags

Flag	Description
s	Static translation slot
d	Dump translation slot on next cleaning cycle
r	Port map translation (Port Address Translation)
n	No randomization of TCP sequence number
i	Inside address translation
D	DNS A RR rewrite
I	Identity translation from **nat 0**

Note When the **vpnclient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

Examples

The following is sample output from the **show xlate** command. It shows how translation slot information with three active PATs.

```
hostname# show xlate

3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

The following is sample output from the **show xlate detail** command.It shows the translation type and interface information with three active PATs.

The first entry is a TCP PAT for host port (10.1.1.15, 1025) on the inside network to host-port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The second entry is a UDP PAT for host port (10.1.1.15, 1028) on the inside network to host port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The third entry is an ICMP PAT for host-ICMP-id (10.1.1.15, 21505) on the inside network to host-ICMP-id (192.150.49.1, 0) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address ICMP ID.

The inside address fields appear as source addresses on packets traversing from the more secure interface to the less secure interface. They appear as destination addresses on packets traversing from the less secure interface to the more secure interface.

```
hostname# show xlate detail

3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

The following is sample output from the **show xlate** command. It shows two static translations. The first translation has one associated connection (called “nconns”), and the second translation has four associated connections.

```
hostname# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

Related Commands

Command	Description
clear xlate	Clears current translation and connection information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show uauth	Displays the currently authenticated users.

CHAPTER 31

shun through sysopt radius ignore-secret Commands

shun

To block connections from an attacking host, use the **shun** command in privileged EXEC mode. To disable a shun, use the **no** form of this command.

shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *src_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of the connection causing the shun.
dst_ip	(Optional) Specifies the address of the target host.
protocol	(Optional) Specifies the IP protocol, such as UDP or TCP. By default, the protocol is 0 (any protocol).
src_ip	Specifies the address of the attacking host.
src_port	(Optional) Specifies the source port of the connection causing the shun.
vlan_id	(Optional) Specifies the VLAN ID.

Defaults

The default protocol is 0 (any protocol).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **shun** command lets you block connections from an attacking host. Packets matching the values in the command are dropped and logged until the blocking function is removed manually or by the Cisco IPS sensor. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you narrow the shun to connections that match those parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the security appliance configuration.

Whenever an interface is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (using the same name), then you must add that interface to the IPS sensor if you want the IPS sensor to monitor that interface.

Examples

The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the security appliance connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

Apply the **shun** command using the following options:

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the connection from the security appliance connection table and also prevents packets from 10.1.1.27:555 to 10.2.2.89:666 (TCP) from going through the security appliance.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

Related Commands

shutdown

To disable an interface, use the **shutdown** command in interface configuration mode. To enable an interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

All physical interfaces are shut down by default. Allocated interfaces in security contexts are not shut down in the configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Note This command only disables the software interface. The physical link remains up, and the directly connected device is still recognized as being up even when the corresponding interface is configured with the **shutdown** command.

Examples\

The following example enables a main interface:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example shuts down the subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.

shutdown (ca-server mode)

To disable the local Certificate Authority (CA) server and render the enrollment interface inaccessible to users, use the **shutdown** command in CA server configuration mode. To enable the CA server, lock down the configuration from changes, and to render the enrollment interface accessible, use the **no** form of this command.

[no] shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

Initially, by default, the CA server is shut down.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command in CA server mode is similar to the **shutdown** command in interface mode. At setup time, the local CA server is shutdown by default and must be enabled using the **no shutdown** command. When you use the **no shutdown** command for the first time, you enable the CA server and generate the CA server certificate and keypair.

Note The CA configuration cannot be changed once you lock it and generate the CA certificate by issuing the **no shutdown** command.

To enable the CA server and lock down the current configuration with the **no shutdown** command, a 7-character password is required to encode and archive a PKCS12 file containing the CA certificate and keypair that is to be generated. The file is stored to the storage identified by a previously specified **database path** command.

Examples

The following example disables the local CA server and renders the enrollment interface inaccessible:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# shutdown
hostname(config-ca-server)#
```

The following example enables the local CA server and makes the enrollment interface accessible:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no shutdown
hostname(config-ca-server)#

hostname(config-ca-server)# no shutdown

% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password: caserver

Re-enter password: caserver

Keypair generation process begin. Please wait...

hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
show crypto ca server	Displays the status of the CA configuration.

sla monitor

To create an SLA operation, use the **sla monitor** command in global configuration mode. To remove the SLA operation, use the **no** form of this command.

sla monitor *sla_id*

no sla monitor *sla_id*

Syntax Description

sla_id	Specifies the ID of the SLA being configured. If the SLA does not already exist, it is created. Valid values are from 1 to 2147483647.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **sla monitor** command creates SLA operations and enters SLA Monitor configuration mode. Once you enter this command, the command prompt changes to `hostname(config-sla-monitor)#` to indicate that you are in SLA Monitor configuration mode. If the SLA operation already exists, and a type has already been defined for it, then the prompt appears as `hostname(config-sla-monitor-echo)#`. You can create a maximum of 2000 SLA operations. Only 32 SLA operations may be debugged at any time.

The **no sla monitor** command removes the specified SLA operation and the commands used to configure that operation.

After you configure an SLA operation, you must schedule the operation with the **sla monitor schedule** command. You cannot modify the configuration of the SLA operation after scheduling it. To modify the the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

To display the current configuration settings of the operation, use the **show sla monitor configuration** command. To display operational statistics of the SLA operation, use the **show sla monitor operation-state command**. To see the SLA commands in the configuration, use the **show running-config sla monitor** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor schedule	Schedules the SLA operation.
timeout	Sets the amount of time the SLA operation waits for a response.
track rtr	Creates a tracking entry to poll the SLA.

sla monitor schedule

To schedule an SLA operation, use the **sla monitor schedule** command in global configuration mode. To remove SLA operation schedule, and place the operation in the pending state, use the **no** form of this command.

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

Syntax Description

after *hh*:*mm*:*ss*	Indicates that the operation should start the specified number of hours, minutes, and seconds after the command was entered.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. After an SLA operation ages out, it is removed from the running configuration.
day	Number of the day to start the operation on. Valid values are from 1 to 31. If a day is not specified, then the current day is used. If you specify a day you must also specify a month.
hh:*mm*[:*ss*]	Specifies an absolute start time in 24-hour notation. Seconds are optional. The next time the specified time occurs is implied unless you specify a *month* and a *day*.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Sets the number of seconds the operation actively collects information.
month	(Optional) Name of the month to start the operation in. If a month is not specified, then the current month is used. I f you specify a month you must also specify a day. You can enter the full English name of the month or just the first three letters.
now	Indicates that the operation should start as soon as the command is entered.
pending	Indicates that no information is collected. This is the default state.
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.
sla-id	The ID of the SLA operation being scheduled.
start-time	Sets the time when the SLA operation starts.

Defaults

The defaults are as follows:

- SLA operations are in the **pending** state until the scheduled time is met. This means that the operation is enabled but not actively collecting data.
- The default **ageout** time is 0 seconds (never ages out).
- The default **life** is 3600 seconds (one hour).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When an SLA operation is in an active state, it immediately begins collecting information. The following time line shows the age-out process of the operation:

```
W---------------------X---------------------Y---------------------Z
```

- W is the time the SLA operation was configured with the **sla monitor** command.
- X is the start time of the SLA operation. This is when the operation became “active”.
- Y is the end of life as configured with the **sla monitor schedule** command (the **life** seconds have counted down to zero).
- Z is the age out of the operation.

The age out process, if used, starts counting down at W, is suspended between X and Y, and is reset to its configured size are starts counting down again at Y. When an SLA operation ages out, the SLA operation configuration is removed from the running configuration. It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation configuration time and start time (X and W) must be less than the age-out seconds.

The **recurring** keyword is only supported for scheduling single SLA operations. You cannot schedule multiple SLA operations using a single **sla monitor schedule** command. The **life** value for a recurring SLA operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the recurring option is not specified, the operations are started in the existing normal scheduling mode.

You cannot modify the configuration of the SLA operation after scheduling it. To modify the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

Examples

The following example shows SLA operation 25 scheduled to begin actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity. When this SLA operation ages out, all configuration information for the SLA operation is removed from the running configuration.

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

The following example shows SLA operation 1 schedule to begin collecting data after a 5-minute delay. The default life of one hour applies.

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

The following example shows SLA operation 3 scheduled to begin collecting data immediately and is scheduled to run indefinitely:

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

The following example shows SLA operation 15 scheduled to begin automatically collecting data every day at 1:30 a.m.:

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor	Defines an SLA monitoring operation.

smart-tunnel auto-signon enable

To enable smart tunnel auto sign-on in clientless (browser-based) SSL VPN sessions, use the **smart-tunnel auto-signon enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

[**no**] **smart-tunnel auto-signon enable** *list* [**domain** *domain*]

To remove the **smart-tunnel auto-signon enable** command from the group policy or username and inherit it from the default group-policy, use the **no** form of the command.

Syntax Description

list	*list* is the name of a smart tunnel auto sign-on list already present in the security appliance webvpn configuration. To view the smart tunnel auto sign-on list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.
domain *domain*	(Optional). Name of the domain to be added to the username during authentication. If you enter a domain, enter the **use-domain** keyword in the list entries.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn configuration mode	•	—	•	—	—
username webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

You must use the **smart-tunnel auto-signon** *list* command to create a list of servers first. You can assign only one list to a group policy or username.

Examples

The following commands enable the smart tunnel auto sign-on list named HR:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR
hostname(config-group-webvpn)
```

The following command enables the smart tunnel auto sign-on list named HR and adds the domain named CISCO to the username during authentication:

```
hostname(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

The following command removes the smart tunnel auto sign-on list named HR from the group policy and inherits the smart tunnel auto sign-on list command from the default group policy:

```
hostname(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

Related Commands

Command	Description
smart-tunnel auto-signon *list*	Create a list of servers for which to automate the submission of credentials in smart tunnel connections.
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration on the security appliance.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel *list*	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel auto-signon list

To create a list of servers for which to automate the submission of credentials in smart tunnel connections, use the **smart-tunnel auto-signon list** command in webvpn configuration mode.

[**no**] **smart-tunnel auto-signon** *list* [**use-domain**] {**ip** *ip-address* [*netmask*] | **host** *hostname-mask*}

Use this command for each server you want to add to a list. To remove an entry from a list, use the **no** form of the command, specifying both the list and the IP address or hostname, as it appears in the security appliance configuration. To display the smart tunnel auto sign-on list entries, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

To remove an entire list of servers from the security appliance configuration, use the **no** form of the command, specifying only the list.

no smart-tunnel auto-signon *list*

Syntax Description

host	Server to be identified by its host name or wildcard mask.
hostname-mask	Host name or wildcard mask to auto-authenticate to.
ip	Server to be identified by its IP address and netmask.
ip-address [*netmask*]	Sub-network of hosts to auto-authenticate to.
list	Name of a list of remote servers. Use quotation marks around the name if it includes a space. The string can be up to 64 characters. The security appliance creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
use-domain	(Optional) Add the Windows domain to the username if authentication requires it. If you enter this keyword, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies, or usernames.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

Following the population of a smart tunnel auto sign-on list, use the **smart-tunnel auto-signon enable** *list* command in group policy webvpn or username webvpn mode to assign the list.

Examples

The following command adds all hosts in the subnet and adds the Windows domain to the username if authentication requires it:

```
asa2(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0
```

The following command removes that entry from the list:

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

The command shown above also removes the list named HR if the entry removed is the only entry in the list. Otherwise, the following command removes the entire list from the security appliance configuration:

```
asa2(config-webvpn)# no smart-tunnel auto-signon HR
```

The following command adds all hosts in the domain to the smart tunnel auto sign-on list named intranet:

```
asa2(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

The following command removes that entry from the list:

```
asa2(config-webvpn)# no smart-tunnel auto-signon intranet host *.exampledomain.com
```

Related Commands

Command	Description
smart-tunnel auto-signon enable	Enables smart tunnel auto sign-on for the group policy or username specified in the command mode.
smart-tunnel auto-signon enable *list*	Assigns a smart tunnel auto sign-on list to a group policy or username
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smart-tunnel auto-start

To start smart tunnel access automatically upon user login in a clientless (browser-based) SSL VPN session, use the **smart-tunnel auto-start** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel auto-start *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the security appliance webvpn configuration. To view any smart tunnel list entries already present in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn configuration mode	•	—	•	—	—
username webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command requires that you use the **smart-tunnel list** command to create the list of applications first.

Examples

The following commands start smart tunnel access for a list of applications named apps1:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel auto-start apps1
hostname(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel commands from the default group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel disable

To prevent smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel disable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel disable

To remove a **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn configuration mode	•	—	•	—	—
username webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

By default, smart tunnels are not enabled, so the **smart-tunnel disable** command is necessary only if the (default) group policy or username configuration contains a **smart-tunnel auto-start** or **smart-tunnel enable** command that you do not want applied for the group policy or username in question.

Examples

The following commands prevent smart tunnel access:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel disable
hostname(config-group-webvpn)
```

Related Commands

Command	Description
`smart-tunnel auto-start`	Starts smart tunnel access automatically upon user login.
`smart-tunnel enable`	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
`smart-tunnel list`	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel enable

To enable smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel enable *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the security appliance webvpn configuration. To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn configuration mode	•	—	•	—	—
username webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **smart-tunnel enable** command assigns a list of applications eligible for smart tunnel access to a group policy or username. It requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the clientless-SSL-VPN portal page. Alternatively, you can use the **smart-tunnel auto-start** command to start smart tunnel access automatically upon user login.

Both commands require that you use the **smart-tunnel list** command to create the list of applications first.

Examples

The following commands enable the smart tunnel list named apps1:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# smart-tunnel enable apps1
hostname(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel list from the default group policy:

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# no smart-tunnel
hostname(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel list

To populate a list of applications that can use a clientless (browser-based) SSL VPN session to connect to private sites, use the **smart-tunnel list** command in webvpn configuration mode.

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]

To remove an application from a list, use the **no** form of the command, specifying the entry. To remove an entire list of applications from the security appliance configuration, use the **no** form of the command, specifying only the list.

no smart-tunnel list *list*

Syntax Description

list	Name of a list of applications or programs. Use quotation marks around the name if it includes a space. The CLI creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
application	Name of the application to be granted smart tunnel access. The string can be up to 64 characters.
path	For Mac OS, the full path to the application. For Windows, the filename of the application; or a full or partial path to the application, including its filename. The string can be up to 128 characters.
platform *OS*	(Optional if the OS is Microsoft Windows) Enter **windows or mac** to specify the host of the application.
hash	(Optional and applicable only for Windows) To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/. After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1** *application* at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash. The SHA-1 hash is always 40 hexadecimal characters.

Defaults

Windows is the default platform.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	Added **platform** *OS*.

Usage Guidelines

You can configure more than one smart tunnel list on a security appliance, but you cannot assign more than one smart tunnel list to a given group policy or username. To populate a smart tunnel list, enter the **smart-tunnel list** command once for each application, entering the same *list* string, but specifying an *application* and *path* that is unique for the OS. Enter the command once for each *OS* you want the list to support.

The session ignores a list entry if the OS does not match the one indicated in the entry. It also ignores an entry if the path to the application is not present.

To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

The *path* must match the one on the computer, but it does not have to be complete. For example, the *path* can consist of nothing more than the executable file and its extension.

Smart tunnels have the following requirements:

- The remote host originating the smart tunnel connection must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
- Users of Microsoft Windows Vista who use smart tunnels or port forwarding must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer's vulnerability to attack.
- The browser must be enabled with Java, Microsoft ActiveX, or both.
- Smart tunnel support for Mac OS requires Safari 3.1.1 or later.

On Microsoft Windows, only Winsock 2, TCP-based applications are eligible for smart tunnel access.

On Mac OS, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel. The following types of applications do not work over a smart tunnel:

- Applications using dlopen or dlsym to locate libsocket calls
- Statically linked applications to locate libsocket calls
- Mac OS applications that use two-level name spaces.
- Mac OS, console-based applications, such as Telnet, SSH, and cURL.
- The PowerPC MAC operating system is not supported with smart tunnel.

On Mac OS, only applications started from the portal page can establish smart tunnel sessions. This requirement includes smart tunnel support for Firefox.Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named csco_st. If this user profile is not present, the session prompts the user to create one.

The following limitations apply to smart tunnels:

- If the remote computer requires a proxy server to reach the security appliance, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. In this configuration, smart tunnels support only basic authentication.

- The security appliance does not support the Microsoft Outlook Exchange (MAPI) proxy. Neither the smart tunnel feature nor port forwarding supports MAPI. For Microsoft Outlook Exchange communication using the MAPI protocol, remote users must use AnyConnect.
- The smart tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library on a Microsoft Windows OS. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.
- A group policy or local user policy supports no more than one list of applications eligible for smart tunnel access and one list of smart tunnel auto sign-on servers.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

Note A sudden problem with smart tunnel access may be an indication that a *path* value is not up-to-date with an application upgrade. For example, the default path to an application typically changes following the acquisition of the company that produces the application and the next upgrade.

Entering a hash provides a reasonable assurance that clientless SSL VPN does not qualify an illegitimate file that matches the string you specified in the *path*. Because the checksum varies with each version or patch of an application, the *hash* you enter can only match one version or patch on the remote host. To specify a *hash* for more than one version of an application, enter the **smart-tunnel list** command once for each version, entering the same *list* string, but specifying the unique *application* string and unique *hash* value in each command.

Note You must maintain the smart tunnel list in the future if you enter *hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a *hash*.

Following the configuration of a smart tunnel list, use the **smart-tunnel auto-start** or **smart-tunnel enable** command to assign the list to group policies or usernames.

Examples

The following command adds a Microsoft Windows application named connect.exe to a smart tunnel list named apps1:

```
hostname(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

The following command adds the Windows application msimn.exe and requires that the hash of the application on the remote host match the last string entered to qualify for smart tunnel access:

```
hostname(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

The following command provides smart tunnel support for the Mac OS browser Safari:

```
hostname(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

Related Commands

Command	Description
`show running-config webvpn smart-tunnel`	Displays the smart tunnel configuration on the security appliance.
`smart-tunnel auto-start`	Starts smart tunnel access automatically upon user login.
`smart-tunnel disable`	Prevents smart tunnel access.
`smart-tunnel enable`	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smartcard-removal-disconnect

To disconnect or retain an IPsec client session if the smart card is removed from the user's computer, use the **smartcard-removal-disconnect** command in group-policy configuration mode.

smartcard-removal-disconnect {**enable** | **disable**}

To remove the **smartcard-removal-disconnect** command from the group policy and inherit the setting from the default group-policy, use the **no** form of the command.

no smartcard-removal-disconnect

Syntax Description

enable	Terminates the IPsec client session if the smart card is removed from the user's computer.
disable	Lets the IPsec client session continue even if the smart card is removed from the user's computer.

Defaults

enable

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy configuration mode	•	—	•	—	—

Command History

Release	Modification
7.0(2)	This command was introduced.

Usage Guidelines

By default, the IPsec client session disconnects if the smart card used for authentication is removed. Enter the **smartcard-removal-disconnect disable** command if you do not want to require users to keep their smart cards in the computer for the duration of the connection.

Examples

The following command lets the client session continue even if the smart card is removed from the user's computer:

```
hostname(config-group-policy)# smartcard-removal-disconnect disable
hostname(config-group-policy)
```

The following command terminates the client session if the smart card is removed from the user's computer:

```
hostname(config-group-policy)# smartcard-removal-disconnect enable
```

smtp from-address

To specify the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server (such as distribution of one-time passwords) use the **smtp from-address** command in CA server configuration mode. To reset the e-mail address to the default, use the **no** form of this command.

smtp from-address *e-mail_address*

no smtp from-address

Syntax Description

e-mail_address	Specifies the e-mail address appearing in the From: field of all e-mails generated by the CA server.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies that the From: field of all e-mails from the local CA server include ca-admin@asa1-ca.example.com:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address ca-admin@asa1-ca.example.com
hostname(config-ca-server)#
```

The following example resets the From: field of all e-mails from the local CA server to the default address admin@asa1-ca.example.com:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp from-address admin@asa1-ca.example.com
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp subject	Customizes the text to appear in the subject field of all e-mails generated by the local CA server.

smtp subject

To customize the text that appears in the subject field of all e-mails generated by the local Certificate Authority (CA) server (such as distribution of one-time passwords), use the **smtp subject** command in CA server configuration mode. To reset the text to the default, use the **no** form of this command.

smtp subject *subject-line*

no smtp subject

Syntax Description

subject-line	Specifies the text appearing in the Subj: field of all e-mails sent from the CA server. The maximum number of characters is 127.

Defaults

By default, the text in the Subj: field is “Certificate Enrollment Invitation”.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example specifies that the text *Action: Enroll for a certificate* appear in the Subj: field of all e-mails from the CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# smtp subject Action: Enroll for a certificate
hostname(config-ca-server)#
```

The following example resets the Subj: field text for all e-mails from the CA server to the default text “Certificate Enrollment Invitation”:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no smtp subject
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server.

smtps

To enter SMTPS configuration mode, use the **smtps** command in global configuration mode. To remove any commands entered in SMTPS command mode, use the **no** version of this command. SMTPS is a TCP/IP protocol that lets you to send e-mail over an SSL connection.

smtps

no smtps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to enter SMTPS configuration mode:

```
hostname(config)# smtps
hostname(config-smtps)#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
show running-config smtps	Displays the running configuration for SMTPS.

smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command.

The security appliance includes an internal SMTP client that the Events system can use to notify external entities that a certain event has occurred. You can configure SMTP servers to receive these event notices, and then forward them to specified e-mail addresses. The SMTP facility is active only when you enable E-mail events an the security appliance.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

Syntax Description

primary_server	Identifies the primary SMTP server. Use either an IP address or DNS name
backup_server	Identifies a backup SMTP server to relay event messages in the event the primary SMTP server is unavailable. Use either an IP address or DNS name.

Defaults

No SMTP server is configured by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set an SMTP server with an IP address of 10.1.1.24, and a backup SMTP server with an IP address of 10.1.1.34:

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-map

To identify a specific map for defining the parameters for SNMP inspection, use the **snmp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

snmp-map *map_name*

no snmp-map *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **snmp-map** command to identify a specific map to use for defining the parameters for SNMP inspection. When you enter this command, the system enters the SNMP map configuration mode, which lets you enter the different commands used for defining the specific map. After defining the SNMP map, you use the **inspect snmp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
```

```
hostname(config-pmap-c)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enables SNMP application inspection.
policy-map	Associates a class map with specific security actions.

snmp-server community

To set the SNMP community string, use the **snmp-server community** command in global configuration mode. To remove the community string, use the **no** form of this command.

snmp-server community *text*

no snmp-server community [*text*]

Syntax Description

text	Sets the community string.

Defaults

The community string is **public**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. The security appliance uses a key to determine whether the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the routers, security appliance, and the management station with this same string. The security appliance uses this string and does not respond to requests with an invalid community string.

Examples

The following example sets the community string to wallawallabingbang:

```
hostname(config)# snmp-server community wallawallabingbang
```

Related Commands

Command	Description
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server contact

To set the SNMP server contact name, use the **snmp-server contact** command in global configuration mode. To remove the SNMP contact name, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact [*text*]

Syntax Description

text	Specifies the name of the contact person or the security appliance system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example sets the SNMP server contact as Pat Johnson:

```
hostname(config)# snmp-server contact Pat Johnson
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable

To enable the SNMP server on the security appliance, use the **snmp-server enable** command in global configuration mode. To disable the SNMP server, use the **no** form of this command.

snmp-server enable

no snmp-server enable

Syntax Description

This command has no arguments or keywords.

Defaults

The SNMP server is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command lets you enable and disable SNMP easily, without having to configure and reconfigure the SNMP traps or other configuration.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as system messages.

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.

Command	Description
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable traps

To enable the security appliance to send traps to the NMS, use the **snmp-server enable traps** command in global configuration mode. To disable traps, use the **no** form of this command.

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

Syntax Description

all	Enables all traps.
entity [*trap*]	Enables entity traps. Traps for **entity** include: • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	Enables IPSec traps. Traps for **ipsec** include: • **start** • **stop**
remote-access [*trap*]	Enables remote access traps. Traps for remote-access include: • **session-threshold-exceeded**
snmp [*trap*]	Enables SNMP traps. By default, all SNMP traps are enabled. Traps for **snmp** include: • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	Enables system log message traps.

Defaults

The default configuration has all **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, the **clear configure snmp-server** command restores the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.)

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

To send traps to the NMS, enter the **logging history** command, and enable logging using the **logging enable** command.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as system messages.

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server group

To configure a new SNMP group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

no snmp-server group *group-name* {**v3** {**auth** | **noauth** | **priv**}}

Syntax Description

auth	Specifies packet authentication without encryption.
group-name	Specifies the name of the group.
noauth	Specifies no packet authentication.
priv	Specifies packet authentication with encryption.
v3	Specifies that the group is using the SNMP Version 3 security model, which is the most secure of the supported security models. This version allows you to explicitly configure authentication characteristics.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(5)	This command was introduced.

Usage Guidelines

To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host. You must also specify Version 3 and a security level. When a community string is configured internally, two groups with the name “public” are automatically created—one for the Version 1 security model and one for the Version 2c security model. When you delete a community string, both configured groups are automatically deleted.

Note A user that is configured to belong to a certain group should have the same security model as the group.

Examples

The following example show how the security appliance can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP configuration counters.
snmp-server host	Sets the SNMP host address.
snmp-server user	Creates a new SNMP user.

snmp-server host

To specify the NMS that can use SNMP on the security appliance, use the **snmp-server host** command in global configuration mode. To disable the NMS, use the **no** form of this command.

snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username***}**] [**udp-port** *port*]

no snmp-server host {*interface* {*hostname* | *ip_address*}} [**trap** | **poll**] [**community** *0* | *8* *community-string*] [**version** {**1** | **2c** | **3** *username***}**] [**udp-port** *port*]

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) community string will follow.
8	Specifies that an encrypted community string will follow.
community	Specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. Valid only for SNMP Version 1 or 2c.
community-string	Specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters. Can be in encrypted or unencrypted (clear text) format.
hostname	Specifies the SNMP notification host, which is usually an NMS or SNMP manager.
interface	Specifies the interface name through which the NMS communicates with the security appliance.
ip_address	Specifies the IP address of an NMS to which SNMP traps should be sent or from which the SNMP requests come. Supports *only* IPv4 addresses.
poll	(Optional) Specifies that the host is allowed to browse (poll), but no traps can be sent.
port	Sets the UDP port number of the NMS host.
trap	(Optional) Specifies that only traps can be sent, and that this host is not allowed to browse (poll).
udp-port	(Optional) Specifies that SNMP traps must be sent to an NMS host on a non-default port.

Defaults

The default UDP port is 162.

The default version is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.
8.0(5)	Support for encrypted passwords was added.

Usage Guidelines

You can specify up to 32 NMSs. If you configure the **snmp-server host** command on a port that is currently in use, the following message appears:

Warning **The UDP port *port* is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Examples

To use the Version 3 security model, you must configure an SNMP group first, then an SNMP user, and then an SNMP host. The username must already be configured on the device. When a device is configured as the standby unit of a failover pair, the SNMP engine ID and user configuration are replicated from the active unit. This action allows a transparent switchover from an SNMP Version 3 query perspective. No configuration changes are necessary in the NMS to accommodate a switchover event.

After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible.

The encrypted community string is always generated by the security appliance; you normally enter the clear text form.

During bootup or upgrade of the security appliance, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Note If you downgrade from version 8.0(5) to a lower version of the security appliance software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

The following example sets the host to 10.1.2.42 attached to the perimeter interface:

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

The following example show how the security appliance can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
hostname(config)# snmp-server group v3 vpn-group priv
hostname(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
hostname(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

The following example sets the host to use an encrypted community string:

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

The following example sets the host to use an unencrypted community string:

```
hostname(config)# snmp-server host mgmt 1.2.3.4 community 0 cisco
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server listen-port

To set the listening port for SNMP requests, use the **snmp-server listen-port** command in global configuration mode. To restore the default port, use the **no** form of the command.

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

Syntax Description

lport	The port on which incoming requests will be accepted. The default port is 161[1].

1. The **snmp-server listen-port** command is only available in admin context, and is not available in the system context.

Defaults

The default port is 161.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:

Warning **The UDP port *port* is in use by another feature. SNMP requests to the device will fail until the snmp-server listen-port command is configured to use a different port.**

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Examples

The following example sets the listening port to 192:

```
hostname(config)# snmp-server listen-port 192
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the security appliance location for SNMP, use the **snmp-server location** command in global configuration mode. To remove the location, use the **no** form of this command.

snmp-server location *text*

no snmp-server location [*text*]

Syntax Description

location *text*	Specifies the security appliance location. The **location** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example sets the security appliance location for SNMP as Building 42, Sector 54:

```
hostname(config)# snmp-server location Building 42, Sector 54
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.

snmp-server user

To configure a new SNMP user, use the **snmp-server user** command in global configuration mode. To remove a specified SNMP user, use the **no** form of this command.

snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

no snmp-server user *username group-name* {**v3** [encrypted] [auth {md5 | sha} *auth-password]*} [priv {**des** | **3des** | **aes** {**128** | **192** | **256**}} *priv-password*]

Syntax Description

128	(Optional) Specifies the use of the 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of the 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of the 256-bit AES algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the AES algorithm for encryption.
auth	(Optional) Specifies which authentication level should be used.
auth-password	(Optional) Specifies a string that enables the agent to receive packets from the host. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
des	(Optional) Specifies the use of the 56-bit DES algorithm for encryption.
encrypted	(Optional) Specifies whether or not the password appears in encrypted format. Encrypted passwords must be in hexadecimal format.
group-name	Specifies the name of the group to which the user belongs.
md5	(Optional) Specifies the HMAC-MD5-96 authentication level.
priv	Specifies packet authentication with encryption.
priv-password	(Optional) Specifies a string that indicates the privacy user password. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
username	Specifies the name of the user on the host that connects to the agent.
v3	Specifies that the SNMP Version 3 security model should be used. Allows the use of the **encrypted, priv,** or **auth** keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(5)	This command was introduced.

Usage Guidelines

An SNMP user must be part of an SNMP group. To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host.

Note If you forget a password, you cannot recover it, and must reconfigure the user.

When the snmp-server user configuration is displayed on the console or written to a file (for example, the startup-configuration file), the localized authentication and privacy digests always appear instead of a plain-text password. This usage is required by RFC 3414, Section 11.2.

Note You must have a 3DES or AES feature license to configure users with the 3DES or AES algorithm.

During bootup or upgrade of the security appliance, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Examples

The following example show how the security appliance can receive SNMP requests using the SNMP Version 3 security model:

```
hostname(config)# snmp-server group engineering v3 auth
hostname(config)# snmp-server user engineering v3 auth sha mypassword
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
snmp-server enable	Enables SNMP on the security appliance.
snmp-server group	Creates a new SNMP group.
snmp-server host	Sets the SNMP host address.

software-version

To identify the Server and User-Agent header fields, which expose the software version of either a server or an endpoint, use the **software-version** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

software-version action {**mask** | **log**} [**log**}

no software-version action {**mask** | **log**} [**log**}

Syntax Description

mask	Masks the software version in the SIP message.
log	Specifies standalone or additional log in case of violation.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to identify the software version in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

speed

To set the speed of a copper (RJ-45) Ethernet interface, use the **speed** command in interface configuration mode. To restore the speed setting to the default, use the **no** form of this command.

speed {**auto** | **10** | **100** | **1000 | nonegotiate**}

no speed [**auto** | **10** | **100** | **1000 | nonegotiate**]

Syntax Description

10	Sets the speed to 10BASE-T.
100	Sets the speed to 100BASE-T.
1000	Sets the speed to 1000BASE-T. For copper Gigabit Ethernet only.
auto	Auto detects the speed.
nonegotiate	For fiber interfaces, sets the speed to 1000 Mbps and does not negotiate link parameters. This command and the **no** form of this command are the only settings available for fiber interfaces. When you set the value to **no speed nonegotiate** (the default), the interface enables link negotiation, which exchanges flow-control parameters and remote fault information.

Defaults

For copper interfaces, the default is **speed auto**.

For fiber interfaces, the default is **no speed nonegotiate**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the speed on the physical interface only.

If your network does not support auto detection, set the speed to a specific value.

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the speed to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the speed to 1000BASE-T:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
duplex	Sets the duplex mode.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.

split-dns

To enter a list of domains to be resolved through the split tunnel, use the **split-dns** command in group-policy configuration mode. To delete a list, use the **no** form of this command.

To delete all split tunneling domain lists, use the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns none** command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, use the **split-dns none** command.

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

Syntax Description

value *domain-name*	Provides a domain name that the security appliance resolves through the split tunnel.
none	Indicates that there is no split DNS list. Sets a split DNS list with a null value, thereby disallowing a split DNS list. Prevents inheriting a split DNS list from a default or specified group policy.

Defaults

Split DNS is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.).

The **no split-dns** command, when used without arguments, deletes all current values, including a null value created by issuing the **split-dns none** command.

Neither the AnyConnect VPN Client nor the SSL VPN Client supports split DNS.

Examples

The following example shows how to configure the domains Domain1, Domain2, Domain3 and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form

split-horizon

To reenable EIGRP split horizon, use the **split-horizon** command in interface configuration mode. To disable EIGRP split horizon, use the **no** form of this command.

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.

Defaults

The **split-horizon** command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For networks that include links over X.25 packet-switched networks, you can use the **neighbor** command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

In general, it is best that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. If split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables EIGRP split horizon on interface Ethernet0/0:

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# no split-horizon eigrp 100
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. This deletes all configured network lists, including a null list created by issuing the **split-tunnel-network-list none** command.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

Syntax Description

value *access-list name*	Identifies an access list that enumerates the networks to tunnel or not tunnel.
none	Indicates that there is no network list for split tunneling; the security appliance tunnels all traffic. Sets a split tunneling network list with a null value, thereby disallowing split tunneling. Prevents inheriting a default split tunneling network list from a default or specified group policy.

Defaults

By default, there are no split tunneling network lists.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance makes split tunneling decisions on the basis of a network list, which is a standard ACL that consists of a list of addresses on the private network.

The **no split-tunnel-network-list** command, when used without arguments, deletes all current network lists, including a null value created by issuing the **split-tunnel-network-list none** command.

Examples

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form.

split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the split-tunnel-policy attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for split tunneling from another group policy.

Split tunneling lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, packets not bound for destinations on the other side of the IPSec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies this split tunneling policy to a specific network.

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option applies only to the Cisco VPN Client.
split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the security appliance. Remote users reach internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's internet service provider.

Defaults

Split tunneling is disabled by default, which is tunnelall.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable split tunneling.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.

spoof-server

To substitute a string for the server header field for HTTP protocol inspection, use the **spoof-server** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

spoof-server *string*

no spoof-server *string*

Syntax Description

string	String to substitute for the server header field. 82 characters maximum.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

WebVPN streams are not subject to the **spoof-server** comand.

Examples

The following example shows how to substitute a string for the server header field in an HTTP inspection policy map:

```
hostname(config-pmap-p)# spoof-server string
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

sq-period

To specify the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture, use the **sq-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of this command.

sq-period *seconds*

no sq-period [*seconds*]

Syntax Description

seconds	Number of seconds between each successful posture validation. The range is 30 to 1800.

Defaults

The default value is 300.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	"nac-" removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance starts the status query timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a *status query.*

Examples

The following example changes the value of the status query timer to 1800 seconds:

```
hostname(config-nac-policy-nac-framework)# sq-period 1800
hostname(config-nac-policy-nac-framework)
```

The following example removes the status query timer from the NAC Framework policy:

```
hostname(config-nac-policy-nac-framework)# no sq-period
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
`nac-policy`	Creates and accesses a Cisco NAC policy, and specifies its type.
`nac-settings`	Assigns a NAC policy to a group policy.
`eou timeout`	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
`reval-period`	Specifies the interval between each successful posture validation in a NAC Framework session.
`debug eap`	Enables logging of Extensible Authentication Protocol events to debug NAC Framework messaging.

ssh

To add SSH access to the security appliance, use the **ssh** command in global configuration mode. To disable SSH access to the security appliance, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

Syntax Description

interface	The security appliance interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface.
ip_address	IPv4 address of the host or network authorized to initiate an SSH connection to the security appliance. For hosts, you can also enter a host name.
ipv6_address/*prefix*	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the security appliance.
mask	Network mask for *ip_address*.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ssh** *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the security appliance. You can have multiple ssh commands in the configuration. The **no** form of the command removes a specific SSH command from the configuration. Use the **clear configure ssh** command to remove all SSH commands.

Before you can begin using SSH to the security appliance, you must generate a default RSA key using the **crypto key generate rsa** command.

The following security algorithms and ciphers are supported on the security appliance:

- 3DES and AES ciphers for data encryption
- HMAC-SHA and HMAC-MD5 algorithms for packet integrity

- RSA public key algorithm for host authentication
- Diffie-Hellman Group 1 algorithm for key exchange

The following SSH Version 2 features are not supported on the security appliance:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

Examples

The following example shows how to configure the inside interface to accept SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

ssh disconnect

To disconnect an active SSH session, use the **ssh disconnect** command in privileged EXEC mode.

ssh disconnect *session_id*

Syntax Description

session_id	Disconnects the SSH session specified by the ID number.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You must specify a session ID. Use the **show ssh sessions** command to obtain the ID of the SSH session you want to disconnect.

Examples

The following example shows an SSH session being disconnected:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

Related Commands

Command	Description
show ssh sessions	Displays information about active SSH sessions to the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh scopy enable

To enable Secure Copy (SCP) on the security appliance, use the **ssh scopy enable** command in global configuration mode. To disable SCP, use the **no** form of this command.

ssh scopy enable

no ssh scopy enable

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

SCP is a server-only implementation; it will be able to accept and terminate connections for SCP but can not initiate them. The security appliance has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the security appliance internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Before initiating the file transfer, the security appliance check available Flash memory. If there is not enough available space, the security appliance terminates the SCP connection. If you are overwriting a file in Flash memory, you still need to have enough free space for the file being copied to the security appliance. The SCP process copies the file to a temporary file first, then copies the temporary file over the file being replaced. If you do not have enough space in Flash to hold the file being copied and the file being overwritten, the security appliance terminates the SCP connection.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address, 10.1.1.1. The idle session timeout is set to 60 minutes, and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh scopy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

ssh timeout

To change the default SSH session idle timeout value, use the **ssh timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

ssh timeout *number*

no ssh timeout

Syntax Description

number	Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes.

Defaults

The default session timeout value is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ssh timeout** command specifies the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes.

Examples

The following example shows how to configure the inside interface to accept only SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.

Command	Description
show ssh sessions	Displays information about active SSH sessions to the security appliance.
ssh disconnect	Disconnects an active SSH session.

ssh version

To restrict the version of SSH accepted by the security appliance, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command. The default values permits SSH Version 1 and SSH Version 2 connections to the security appliance.

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

Syntax Description

1	Specifies that only SSH Version 1 connections are supported.
2	Specifies that only SSH Version 2 connections are supported.

Defaults

By default, both SSH Version 1 and SSH Version 2 are supported.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

1 and 2 specify which version of SSH the security appliance is restricted to using. The **no** form of the command returns the security appliance to the default stance, which is compatible mode (both version can be used).

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.

ssl certificate-authentication

To enable client certificate authentication, use the **ssl certificate-authentication** command in global configuration mode. To disable ssl certificate authentication, use the **no** version of this command.

ssl certificate-authentication interface *interface-name* **port** *port-number*

no ssl certificate-authentication interface *interface-name* **port** *port-numbe***r**

Syntax Description

interface-name	The name of the selected interface, such as inside, management, and outside.
port-number	The TCP port number, an integer in the range 1-65535.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
8.0(3)	This command was introduced.

Usage Guidelines

This command replaces the deprecated http authentication-certificate command.

Examples

The following example shows how to configure the security appliance to use the SSL certificate authentication feature:

```
hostname(config)# ssl certificate-authentication interface inside port 330
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured SSL commands.

ssl client-version

To specify the SSL/TLS protocol version the security appliance uses when acting as a client, use the **ssl client-version** command in global configuration mode. To revert to the default, **any**, use the **no** version of this command. This command lets you restrict the versions of SSL/TLS that the security appliance sends.

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

Syntax Description

any	The security appliance sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3-only	The security appliance sends SSL version 3 hellos, and accepts only SSL version 3.
tlsv1-only	The security appliance sends TLSv1 client hellos, and accepts only TLS version 1.

Defaults

The default value is **any**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

Examples

The following example shows how to configure the security appliance to communicate using only TLSv1 when acting as an SSL client:

```
hostname(config)# ssl client-version tlsv1-only
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
show running-config ssl	Displays the current set of configured SSL commands.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl encryption

To specify the encryption algorithms that the SSL/TLS protocol uses, use the **ssl encryption** command in global configuration mode**.** Issuing the command again overwrites the previous setting. The ordering of the algorithms determines preference for their use. You can add or remove algorithms to meet the needs of your environment. To restore the default, which is the complete set of encryption algorithms, use the **no** version of the command.

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*aes128-sha1*] [*aes256-sha1*] [*possibly others*]

no ssl encryption

Syntax Description

3des-sha1	Specifies triple DES encryption with Secure Hash Algorithm 1.
des-sha1	Specifies DES encryption with Secure Hash Algorithm 1.
rc4-md5	Specifies RC4 encryption with an MD5 hash function.
aes128-sha1	Specifies triple AES 128-bit encryption with Secure Hash Algorithm 1.
aes256-sha1	Specifies triple AES 256-bit encryption with Secure Hash Algorithm 1.
possibly others	Indicates that more encryption algorithms may be added in future releases.

Defaults

The default is to have all algorithms available in the following order:

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ASDM License tab reflects the maximum encryption the license supports, not the value you configure.

Examples

The following example shows how to configure the security appliance to use the 3des-sha1 and des-sha1 encryption algorithms:

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl server-version

To specify the SSL/TLS protocol version the security appliance uses when acting as a server, use the **ssl server-version** command in global configuration mode. To revert to the default, any, use the **no** version of this command. This command lets you restrict the versions of SSL/TSL that the security appliance accepts.

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

Syntax Description

any	The security appliance accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3	The security appliance accepts SSL version 2 client hellos, and negotiates to SSL version 3.
sslv3-only	The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3.
tlsv1	The security appliance accepts SSL version 2 client hellos, and negotiates to TLS version 1.
tlsv1-only	The security appliance accepts only TLSv1 client hellos, and uses only TLS version 1.

Defaults

The default value is **any**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

If you configure e-mail proxy, do not set thhe SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.

Examples

The following example shows how to configure the security appliance to communicate using only TLSv1 when acting as an SSL server:

```
hostname(config)# ssl server-version tlsv1-only
```

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured ssl commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. If you do not specify an interface, this command creates the fallback trustpoint for all interfaces that do not have a trustpoint configured. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** version of this command. To remove an entry that does specify an interface, use the **no ssl trust-point {***trustpoint [interface]***}** version of the command.

ssl trust-point {*trustpoint [interface]***}**

no ssl trust-point

Syntax Description

interface	The name for the interface to which the trustpoint applies. The **nameif** command specifies the name of the interface.
trustpoint	The *name* of the CA trustpoint as configured in the **crypto ca trustpoint** {*name*} command.

Defaults

The default is no trustpoint association. The security appliance uses the default self-generated RSA key-pair certificate.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Observe these guidelines when using this command:

- The value for *trustpoint* must be the name of the CA trustpoint as configured in the **crypto ca trustpoint {*name*}** command.
- The value for *interface* must be the *nameif* name of a previously configured interface.
- Removing a trustpoint also removes any **ssl trust-point** entries that reference that trustpoint.
- You can have one **ssl trustpoint** entry for each interface and one that specifies no interfaces.
- You can reuse the same trustpoint for multiple entries.

The following example explains how to use the **no** versions of this command:

The configuration includes these SSL trustpoints:

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

Issue the command:

no ssl trust-point

Then show run ssl will have:

ssl trust-point tp2 outside

Examples

The following example shows how to configure an ssl trustpoint called FirstTrust for the inside interface, and a trustpoint called DefaultTrust with no associated interface.

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

The next example shows how to use the **no** version of the command to delete a trustpoint that has no associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

The next example shows how to delete a trustpoint that does have an associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.

sso-server

To create a Single Sign-On (SSO) server for security appliance user authentication, use the **sso-server** command in webvpn configuration mode. With this command, you must specify the SSO server type.

To remove an SSO server, use the **no** form of this command.

sso-server *name* **type [***siteminder* | *saml-v1.1-post*]

no sso-server *name*

Note This command is required for SSO authentication.

Syntax Description

name	Specifies the name of the SSO server. Minimum of 4 characters and maximum of 31 characters.
saml-v1.1-post	Specifies that the security appliance SSO server being configured is a SAML, Version 1.1, SSO server of the POST type.
siteminder	Specifies that the security appliance SSO server being configured is a Computer Associates SiteMinder SSO server.
type	Specifies the type of SSO server. SiteMinder and SAML-V1.1-POST are the only types available.

Defaults

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **sso-server** command lets you create an SSO server.

In the authentication, the security appliance acts as a proxy for the WebVPN user to the SSO server. The security appliance currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. Currently, the available arguments for the type option are restricted to *siteminder* or *saml-V1.1-post*.

Examples

The following example, entered in webvpn configuration mode, creates a SiteMinder-type SSO server named “example1”:

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example1 type siteminder
hostname(config-webvpn-sso-siteminder)#
```

The following example, entered in webvpn configuration mode, creates a SAML, Version 1.1, POST-type SSO server named “example2”:

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example2 type saml-v1.1-post
hostname(config-webvpn-sso-saml)#
```

Related Commands

Command	Description
assertion-consumer-url	Identifies the URL for the SAML-type SSO assertion consumer service.
issuer	Specifies the SAML-type SSO server’s security device name.
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
test sso-server	Tests an SSO server with a trial authentication request.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

sso-server value (group-policy webvpn)

To assign an SSO server to a group policy, use the **sso-server value** command in webvpn configuration mode available in group-policy configuration mode.

To remove the assignment and use the default policy, use the **no** form of this command.

To prevent inheriting the default policy, use the **sso-server none** command.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the group policy.

Defaults

The default policy assigned to the group is DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **sso-server value** command, when entered in group-policy webvpn mode, lets you assign an SSO server to a group policy.

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

Note Enter the same command, **sso-server value**, in username-webvpn configuration mode to assign SSO servers to user policies.

Examples

The following example commands create the group policy my-sso-grp-pol and assigns it to the SSO server named example:

```
hostname(config)# group-policy my-sso-grp-pol internal
```

```
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
sso-server value (username webvpn)	Assigns an SSO server to a user policy.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder-type SSO authentication requests.

sso-server value (username webvpn)

To assign an SSO server to a user policy, use the **sso-server value** command in webvpn configuration mode available in username configuration mode.

To remove an SSO server assignment for a user, use the **no** form of this command.

When a user policy inherits an unwanted SSO server assignment from a group policy, use the **sso-server none** command to remove the assignment.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the user policy.

Defaults

The default is for the user policy to use the SSO server assignment in the group policy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

The **sso-server value** command lets you assign an SSO server to a user policy.

Note Enter the same command, **sso-server value**, in group-webvpn configuration mode to assign SSO servers to group policies.

Examples

The following example commands assign the SSO server named my-sso-server to the user policy for a WebVPN user named Anyuser:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value my-sso-server
```

```
hostname(config-username-webvpn)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
sso-server value (config-group-webvpn)	Assigns an SSO server to a group policy.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

start-url

To enter the URL at which to retrieve an optional pre-login cookie, use the **start-url** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

start-url *string*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The URL for an SSO server. The maximum URL length is 1024 characters.

Defaults

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance can use an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The authenticating web server may execute a pre-login sequence by sending a Set-Cookie header along with the login page content. You can discover this by connecting directly to the authenticating web server's login page with your browser. If the web server sets a cookie when the login page loads and if this cookie is relevant for the following login session, you must use the **start-url** command to enter the URL at which the cookie is retrieved. The actual login sequence starts after the pre-login cookie sequence with the form submission to the authenticating web server.

Note The **start-url** command is only required in the presence of the pre-login cookie exchange.

Examples

The following example, entered in aaa-server host configuration mode, specifies a URL for retrieving the pre-login cookie of https://example.com/east/Area.do?Page-Grp1:

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

state-checking

To enforce state checking for H.323, use the **state-checking** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

state-checking [h225 | ras]

no state-checking [h225 | ras]

Syntax Description

h225	Enforces state checking for H.225.
ras	Enforces state checking for RAS.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enforce state checking for RAS on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

static

To configure a persistent one-to-one address translation rule by mapping a real IP address to a mapped IP address, use the **static** command in global configuration mode. To restore the default settings, use the **no** form of this command.

For static NAT:

static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

For static PAT:

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

Syntax Description

access-list *access_list_name*	Identify the real addresses and destination/source addresses using an extended access list. This feature is known as policy NAT.
	
	Create the extended access list using the **access-list extended** command. The first address in the access list is the real address; the second address is either the source or destiniation address, depending on where the traffic originates. For example, to translate the real address 10.1.1.1 to the mapped address 192.168.1.1 when 10.1.1.1 sends traffic to the 209.165.200.224 network, the **access-list** and **static** commands are:
	
	`hostname(config)# access-list TEST extended ip host 10.1.1.1 209.165.200.224 255.255.255.224`
	`hostname(config)# static (inside,outside) 192.168.1.1 access-list TEST`
	
	In this case, the second address is the destination address. However, the same configuration is used for hosts to originate a connection to the mapped address. For example, when a host on the 209.165.200.224 network initiates a connection to 192.168.1.1, then the second address in the access list is the source address.
	
	This access list should include only **permit** ACEs. You can optionally specify the real and destination ports in the access list using the **eq** operator. Policy NAT does not consider the **inactive** or **time-range** keywords; all ACEs are considered to be active for policy NAT configuration.
	
	If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access.

dns	(Optional) Rewrites the A record, or address record, in DNS replies that match this static. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value. **Note** DNS inspection must be enabled to support this functionality.
emb_lim	(Optional) Specifies the maximum number of embryonic connections per host. The default is 0, which means unlimited embryonic connections. Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.
interface	Uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP. **Note** You must use the **interface** keyword instead of specifying the actual IP address when you want to include the IP address of an interface in a static PAT entry.
mapped_ifc	Specifies the name of the interface connected to the mapped IP address network.
mapped_ip	Specifies the address to which the real address is translated.
mapped_port	Specifies the mapped TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers

nailed	(Optional) Allows TCP sessions for asymmetrically routed traffic. This option allows inbound traffic to traverse the security appliance without a corresponding outbound connection to establish the state. This command is used in conjunction with the **failover timeout** command. The **failover timeout** command specifies the amount of time after a system boots or becomes active that the nailed sessions are accepted. If not configured, the connections cannot be reestablished. **Note** Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection. Using the **asr-group** command to configure asymmetric routing support is more secure than using the **static** command with the **nailed** option and is the recommended method for configuring asymmetric routing support.
netmask *mask*	Specifies the subnet mask for the real and mapped addresses. For single hosts, use 255.255.255.255. If you do not enter a mask, then the default mask for the IP address class is used, with one exception. If a host-bit is non-zero after masking, a host mask of 255.255.255.255 is used. If you use the **access-list** keyword instead of the *real_ip*, then the subnet mask used in the access list is also used for the *mapped_ip*.
norandomseq	(Optional) Disables TCP ISN randomization protection. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions. Randomizing the ISN of the protected host prevents an attacker from predecting the next ISN for a new connection and potentially hijacking the new session. TCP initial sequence number randomization can be disabled if required. For example: • If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic. • If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
real_ifc	Specifies the name of the interface connected to the real IP address network.
real_ip	Specifies the real address that you want to translate.
real_port	Specifies the real TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers
tcp	For static PAT, specifies the protocol as TCP.
tcp *max_conns*	Specifies the maximum number of simultaneous TCP connections allowed to the local-host (see the **local-host** command). The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the module policy framework by setting a connection-limit on a class within a policy-map.

udp	For static PAT, specifies the protocol as UDP.
udp *udp_max_conns*	(Optional) Specifies the maximum number of simultaneous UDP connections allowed to the local-host (see the **local-host** command). The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the module policy framework by setting a connection-limit on a class within a policy-map.

Defaults

The default value for *tcp_max_conns*, *emb_limit*, and *udp_max_conns* is 0 (unlimited), which is the maximum available.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2.(1)	NAT is now supported in transparent firewall mode.

Usage Guidelines

Static NAT creates a fixed translation of real address(es) to mapped address(es).With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if there is an access list that allows it).

Note For static policy NAT, in undoing the translation, the ACL in the **static** command is not used. If the destination address in the packet matches the mapped address in the static rule, the static rule is used to untranslate the address.

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if there is an access list that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

Using matching ports is supported for static policy NAT, but it is unsupported for NAT.

Static PAT is the same as static NAT, except it lets you specify the protocol (TCP or UDP) and port for the real and mapped addresses.

This feature lets you identify the same mapped address across many different static statements, so long as the port is different for each statement (you cannot use the same mapped address for multiple static NAT statements).

You cannot use the same real or mapped address in multiple **static** commands between the same two interfaces, unless you use static PAT. Do not use a mapped address in the **static** command that is also defined in a **global** command for the same mapped interface.

When you specify the ports in policy NAT for applications that require application inspection for secondary channels (FTP, VoIP, etc.), the security appliance automatically translates the secondary ports.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access.

After changing or removing a static command statement, use the **clear xlate** command to clear the translations.

You can alternatively configure maximum connections, maximum embryonic connections, and TCP sequence randomization using the **set connection** commands. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

The connection attributes (**dns**, **norandomseq**, **nailed**, **tcp**, and **udp**) have a per-host limit. In some cases, such as policy NAT (with an access list) or NAT involving more than two interfaces, a connection attribute can derive its value from multiple **nat** and **static** commands. In such cases, the value from the rule that matches the first packet is the value that takes precedent. For example, with the following configuration, TCP connection limits of 100 and 200 can be applicable:

```
static (inside,dmz) 192.168.1.1 192.168.1.100 tcp 100
static (inside,outside) 192.168.1.1 192.168.1.100 tcp 200
```

If the first packet from host 192.168.1.1 is toward the dmz interface, the TCP connection limit is 100 for *all* subsequent TCP sessions.

Examples

Static NAT Examples

For example, the following policy static NAT example shows a single real address that is translated to two mapped addresses depending on the destination address:

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

The following command maps an inside IP address (10.1.1.3) to an outside IP address (209.165.201.12):

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255
```

The following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
```

The following command statically maps an entire subnet:

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

This example shows how to permit a finite number of users to call in through H.323 using Intel Internet Phone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, or Microsoft NetMeeting. The **static** command maps addresses 209.165.201.0 through 209.165.201.30 to local addresses 10.1.1.0 through 10.1.1.30 (209.165.201.1 maps to 10.1.1.1, 209.165.201.10 maps to 10.1.1.10, and so on).

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask 255.255.255.224
```

```
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq h323
hostname(config)# access-group acl_out in interface outside
```

This example shows the commands that are used to disable Mail Guard:

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

In the example, the **static** command allows you to set up a global address to permit outside hosts access to the 10.1.1.1 mail server host on the dmz1 interface. You shoud set the MX record for DNS to point to the 209.165.201.1 address so that mail is sent to this address. The **access-list** command allows the outside users to access the global address through the SMTP port (25). The **no fixup protocol** command disables Mail Guard.

Static PAT Examples

For example, for Telnet traffic initiated from hosts on the 10.1.3.0 network to the security appliance outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering the following commands:

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

For HTTP traffic initiated from hosts on the 10.1.3.0 network to the security appliance outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering:

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the security appliance outside interface (10.1.2.14) to the inside host at 10.1.1.15, enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
```

If you want to allow the preceding real Telnet server to initiate connections, though, then you need to provide additional translation. For example, to translate all other types of traffic, enter the following commands. The original **static** command provides translation for Telnet to the server, while the **nat** and **global** commands provide PAT for outbound connections from the server.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

If you also have a separate translation for all inside traffic, and the inside hosts use a different mapped address from the Telnet server, you can still configure traffic initiated from the Telnet server to use the same mapped address as the **static** statement that allows Telnet traffic to the server. You need to create a more exclusive **nat** statement just for the Telnet server. Because **nat** statements are read for the best match, more exclusive **nat** statements are matched before general statements. The following example shows the Telnet **static** statement, the more exclusive **nat** statement for initiated traffic from the Telnet server, and the statement for other inside hosts, which uses a different mapped address.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
```

```
hostname(config)# global (outside) 2 10.1.2.78
```

To translate a well-known port (80) to another port (8080), enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

Related Commands

Command	Description
clear configure static	Removes **static** commands from the configuration.
clear xlate	Clears all translations.
nat	Configures dynamic NAT.
show running-config static	Displays all **static** commands in the configuration.
timeout conn	Sets the timeout for connections.

strict-header-validation

To enable strict validation of the header fields in the SIP messages according to RFC 3261, use the **strict-header-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

no strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection of a violation occurs.
log	Specifies standalone or additional log in case of violation. It can be associated to any of the actions.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable strict validation of SIP header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

strict-http

To allow forwarding of non-compliant HTTP traffic, use the **strict-http** command in HTTP map configuration mode, which is accessible using the **http-map** command. To reset this feature to its default behavior, use the **no** form of the command.

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generate a syslog.
reset	Closes the connection with a TCP reset message to client and server.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the security appliance to allow forwarding of non-compliant HTTP traffic. This command overrides the default behavior, which is to deny forwarding of non-compliant HTTP traffic.

Examples

The following example allows forwarding of non-compliant HTTP traffic:

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

strip-group

This command applies only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the "@" delimiter (juser@abc).

To enable or disable strip-group processing, use the **strip-group** command in tunnel-group general-attributes mode. The security appliance selects the tunnel group for IPSec connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the security appliance sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the security appliance sends the entire username including the realm.

To disable strip-group processing, use the **no** form of this command.

strip-group

no strip-group

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named "remotegrp" for type IPSec remote access, then enters general configuration mode, sets the tunnel group named "remotegrp" as the default group policy, and then enables strip group for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

strip-realm

To enable or disable strip-realm processing, use the **strip-realm** command in tunnel-group general-attributes configuration mode. Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. A realm is an administrative domain appended to a username with the @ delimiter (username@realm). If the command is enabled, the security appliance sends only the user part of the username authorization/authentication. Otherwise, the security appliance sends the entire username.

To disable strip-realm processing, use the **no** form of this command.

strip-realm

no strip-realm

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPSec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip realm for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-realm
```

neral)

ostname(config-ge

Related Commands

h

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups or the specified tunnel-group.
show running-config tunnel-group	Shows the current tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

storage-key

To specify a storage key to protect the date stored between sessions, use the **storage-key** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

storage- key { **none** | **value** <*string*>}

no storage-key

Syntax Description

string	Specifies a string to use as the value of the storage key. This string can be up to 64 characters long.

Defaults

The default is **none**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

While you can use any character except spaces in the storage key value, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z.

Examples

The following example sets the storage key to the value abc123:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-key value abc123
```

Related Commands

Command	Description
storage-objects	Configures storage objects for the data stored between sessions.

storage-objects

To specify which storage objects to use for the data stored between sessions, use the **storage-objects** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

storage- objects { **none** | **value** <*string*>}

no storage-objects

Syntax Description

string	Specifies the name of the storage objects. This string can be up to 64 characters long.

Defaults

The default is **none**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

While you can use any character except spaces and commas in the storage object name, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z. Use a comma, with no space, to separate the names of storage objects in the string.

Examples

The following example sets the storage object names to cookies and xyz456:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-object value cookies,xyz456
```

Related Commands

Command	Description
storage-key	Configures storage key to use for the data stored between sessions.
user-storage	Configures a location for storing user data between sessions

subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject DN of the IPSec peer certificate, use the **subject-name** command in crypto ca certificate map configuration mode. To remove an subject-name, use the **no** form of the command.

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*]

Syntax Description

attr *tag*	Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows: DNQ = DN qualifier GENQ = Generational qualifier I = Initials GN = Given name N = Name SN = Surname IP = IP address SER = Serial number UNAME = Unstructured name EA = Email address T = Title O = Organization Name L = Locality SP = State/Province C = Country OU = Organizational unit CN = Common name
co	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the rule entry string must not be a substring in theDN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the value to be matched.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca certificate map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters the CA certificate map mode for certificate map 1 and creates a rule entry indicating that the Organization attribute of the certificate subject name must be equal to Central.

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
issuer-name	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

subject-name (crypto ca trustpoint)

To include the indicated subject DN in the certificate during enrollment, use the **subject-name** command in crypto ca trustpoint configuration mode. This is the person or system that uses the certificate. To restore the default setting, use the **no** form of the command.

subject-name *X.500_name*

no subject-name

Syntax Description

X.500_name	Defines the X.500 distinguished name. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains commas or spaces. For example: **cn=crl,ou=certs,o="cisco systems, inc.",c=US**. The maximum length is 500 characters.

Defaults

The default setting is not to include the subject name.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and sets up automatic enrollment at the URL https//:frog.phoobin.com and includes the subject DN OU certs in the the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=certs
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment url	Specifies the URL for enrolling with a CA.

subject-name-default

To specify a generic subject-name DN to be appended to the username in all user certificates issued by the local CA server, use the **subject-name-default** command in CA server configuration mode. To reset the subject-name DN to the default value, use the **no** form of this command.

subject-name-default *dn*

no subject-name-default

Syntax Description

dn	Specifies the generic subject-name DN included with a username in all user certificates issued by the local CA server. Supported DN attributes are cn (common name), ou (organizational unit, ol (organization locality), st (state), ea (e-mail address), c (company), t (title), and sn (surname). Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains commas or spaces. The *dn* can be up to 500 characters.

Defaults

This command is not part of the default configuration. This command specifies the default DN in the certificate. The security appliance ignores this command if the user entry has a DN.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **subject-name-default** command specifies a common, generic distinguished name to be used with a username to form a subject name for issued certificates. The *dn* value cn=username is sufficient for this purpose. This command eliminates the need to define a subject-name DN specifically for each user.

The security appliance uses this command only when issuing certificates if a user entry does not specify a DN. The DN field is optional when a user is added using the **crypto ca server user-db add** dn *dn* command.

Examples

The following example specifies a DN:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate, issued certificates, or the CRL.

summary-address (OSPF)

To create aggregate addresses for OSPF, use the **summary-address** command in router configuration mode. To remove the summary address or specific summary address options, use the **no** form of this command.

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
mask	IP subnet mask that is used for the summary route.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Defaults

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix/mask pair are not suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Routes learned from other routing protocols can be summarized. Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

To remove a **summary-address** command from the configuration, use the no form of the command without specifying any of the optional keywords or arguments. To remove an option from a summary command in the configuration, use the **no** form of the command with the options that you want removed. See the "Examples" section for more information.

Examples

The following example configures route summarization with a **tag** set to 3:

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
router ospf	Enters router configuration mode.
show ospf summary-address	Displays the summary address settings for each OSPF routing process.

summary-address (EIGRP)

To configure a summary for EIGRP on a specific interface, use the **summary-address** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

summary-address *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

Syntax Description

as-number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.
addr	The summary IP address.
mask	The subnet mask to apply to the IP address.
admin-distance	(Optional) The administrative distance of the summary route. Valid values are from 0 to 255. If not specified, the default value is 5.

Defaults

The defaults are as follows:

- EIGRP automatically summarizes routes to the network level, even for a single host route.
- The administrative distance of EIGRP summary routes is 5.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

By default, EIGRP summarizes subnet routes to the network level. Use the **no auto-summary** command to disable automatic route summarization. Using the **summary-address** command lets you manually define subnet route summaries on a per-interface basis.

Examples

The following example configures route summarization with a **tag** set to 3:

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

Related Commands

Command	Description
auto-summary	Automatically creates summary addresses for the EIGRP routing process.

sunrpc-server

To create entries in the SunRPC services table, use the **sunrpc-server** command in global configuration mode. To remove SunRPC services table entries from the configuration, use the **no** form of this command.

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **] timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

Syntax Description

ifc_name	Server interface name.
ip_addr	SunRPC server IP address.
mask	Network mask.
port *port* [- *port*]	Specifies the SunRPC protocol port range.
port- *port*	(Optional) Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program number as specified in the **sunrpcinfo** command.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The SunRPC services table is used to allow SunRPC traffic through the security appliance based on an established SunRPC session for the duration specified by the timeout.

Examples

The following example shows how to create an SunRPC services table:

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
show running-config sunrpc-server	Displays the information about the SunRPC configuration.

support-user-cert-validation

To validate a remote user certificate based on the current trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate, use the **support-user-cert-validation** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

support-user-cert-validation

no support-user-cert-validation

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to support user certificate validation.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is automatically disabled if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and enables the trustpoint central to accept user validation:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

svc ask

To enable the security appliance to prompt remote SSL VPN client users to download the client, use the **svc ask** command from group policy webvpn or username webvpn configuration modes.

To remove the command from the configuration, use the no form of the command:

svc ask {**none** | **enable** [**default** {**webvpn** | **svc**} **timeout** *value*]}

no svc ask none [**default** {**webvpn** | **svc**}]

Syntax Description

none	Immediately performs the default action.
enable	Prompts the remote user to download the client or goes to the portal page for clientless connections and waits indefinitely for user response.
default svc timeout *value*	Prompts the remote user to download the client or goes to the portal page for clientless connections, and waits the duration of *value* before taking the default action—downloading the client.
default webvpn timeout *value*	Prompts the remote user to download the client or goes to the portal page for clientless connections, and waits the duration of *value* before taking the default action—displaying the WebVPN portal page.

Defaults

The default for this command is **svc ask none default webvpn**. The security appliance immediately displays the portal page for clientless connections.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

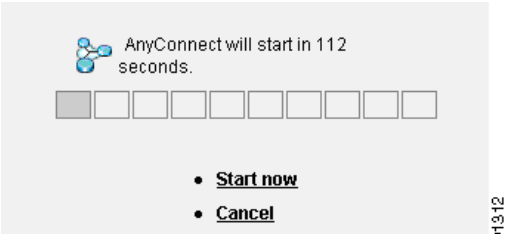
Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Figure 31-1 shows the prompt displayed to remote users when either **default svc timeout** *value* or **default webvpn timeout** *value* is configured:

Figure 31-1 Prompt Displayed to Remote Users for SSL VPN Client Download



Examples

The following example configures the security appliance to prompt the remote user to download the client or go to the portal page and to wait 10 seconds for user response before downloading the client:

```
hostname(config-group-webvpn)# svc ask enable default svc timeout 10
```

Related Commands

Command	Description
show webvpn svc	Displays information about installed SSL VPN clients.
svc	Enables or requires the SSL VPN client for a specific group or user.
svc image	Specifies a client package file that the security appliance expands in cache memory for downloading to remote PCs.

svc compression

To enable compression of http data over an SSL VPN connection for a specific group or user, use the **svc compression** command in group policy webvpn or username webvpn configuration modes.

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command:

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

Syntax Description

deflate	Specifies compression is enabled for the group or user.
none	Specifies compression is disabled for the group or user.

Defaults

By default, compression is set to *none* (disabled).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

For SSL VPN connections, the **compression** command configured from webvpn configuration mode overrides the **svc compression** command configured in group policy and username webvpn modes.

Examples

In the following example, SVC compression is disabled for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

Related Commands

Command	Description
compression	Enables compression for all SSL, WebVPN, and IPSec VPN connections.
show webvpn svc	Displays information about installed SSL VPN clients.

svc dpd-interval

To enable Dead Peer Detection (DPD) on the security appliance and to set the frequency that either the remote client or the security appliance performs DPD over SSL VPN connections, use the **svc dpd-interval** command from group policy or username webvpn mode:

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited.

Syntax Description

gateway *seconds*	Specifies the frequency, from 30 to 3600 seconds, that the security appliance performs DPD.
gateway none	Disables DPD that the security appliance performs.
client *seconds*	Specifies the frequency, from 30 to 3600 seconds, that the client performs DPD.
client none	Disables DPD that the client performs.

Defaults

The default is DPD is enabled and set to 30 seconds for both the security appliance (gateway) and the client.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(3)	The default setting changed from disabled to 30 seconds for both the security appliance (gateway) and the client.

Examples

In the following example, the user configures the DPD frequency performed by the security appliance (gateway) to 3000 seconds, and the DPD frequency performed by the client to 1000 seconds, for the existing group policy *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
```

Related Commands

Command	Description
svc	Enables or requires the SSL VPN client for a specific group or user.
svc keepalive	Specifies the frequency at which a client on a remote computer sends keepalive messages to the security appliance over an SSL VPN connection.
svc keep-installer	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
svc rekey	Enables the client to perform a rekey on an SSL VPN connection.

svc dtls enable

To enable Datagram Transport Layer Security (DTLS) connections on an interface for specific groups or users establishing SSL VPN connections with the Cisco AnyConnect VPN Client, use the **dtls enable** command from group policy webvpn or username attributes webvpn configuration mode.

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command:

dtls enable *interface*

no dtls enable *interface*

Syntax Description

interface	The name of the interface.

Defaults

The default is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Enabling DTLS allows the AnyConnect client establishing an SSL VPN connection to use two simultaneous tunnels—an SSL tunnel and a DTLS tunnel. Using DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

If you do not enable DTLS, AnyConnect client users establishing SSL VPN connections connect only with an SSL tunnel.

This command enables DTLS for specific groups or users. To enable DTLS for all AnyConnect client users, use the **dtls enable** command in webvpn configuration mode.

Examples

The following example enters group policy webvpn configuration mode for the group policy *sales* and enables DTLS:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
```

```
hostname(config-group-webvpn)# svc dtls enable
```

Related Commands

Command	Description
dtls port	Specifies a UDP port for DTLS.
svc dtls	Enables DTLS for groups or users establishing SSL VPN connections.
vpn-tunnel-protocol	Specifies VPN protocols that the security appliance allows for remote access, including SSL.

svc enable

To enable the security appliance to download an SSL VPN client to remote computers, use the **svc enable** command from webvpn configuration mode.

To remove the command from the configuration, use the **no** form of the command:

svc enable

no svc enable

Defaults

The default for this command is disabled. The security appliance does not download the client.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

Entering the **no svc enable** command does not terminate active sessions.

Examples

In the following example, the user enables the security appliance to download the client:

```
(config)# webvpn
(config-webvpn)# svc enable
```

Related Commands

Command	Description
show webvpn svc	Displays information about SSL VPN clients installed on the security appliance and loaded in cache memory for downloading to remote PCs.
svc localization	Specifies the package file used to store localization files that are downloaded to the Cisco AnyConnect VPN Client.
svc profiles	Specifies the name of the file used to store profiles that the security appliance downloads to the Cisco AnyConnect VPN Client.
svc image	Specifies an SSL VPN client package file that the security appliance expands in cache memory for downloading to remote PCs.

svc image

To specify an SSL VPN client package file that the security appliance expands in cache memory for downloading to remote PCs, use the **svc image** command from webvpn configuration mode.

To remove the command from the configuration, use the **no** form of the command:

svc image *filename order* [**regex** *expression*]

no svc image *filename order* [**regex** *expression*]

Syntax Description

filename	Specifies the filename of the package file, up to 255 characters.
order	With multiple client package files, *order* specifies the order of the package files, from 1 to 65535. The security appliance downloads portions of each client, in the order you specify, to the remote PC until it achieves a match with the operating system.
regex *expression*	Specifies a string that the security appliance uses to match against the User-Agent string passed by the browser.

Defaults

The default order is 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.
8.0(1)	The **regex** *expression* argument was added.

Usage Guidelines

Numbering the package files establishes the order in which the security appliance downloads portions of them to the remote PC until it achieves a match with the operating system. It downloads the package file with the lowest number first. Therefore, you should assign the lowest number to the package file that matches the most commonly-encountered operating system used on remote PCs.

The default order is 1. If you do not specify the *order* argument, each time you enter the **svc image** command, you overwrite the image that was previously considered number 1.

You can enter the **svc image** command for each client package file in any order. For example, you can specify the package file to be downloaded second (*order* 2) before entering the **svc image** command specifying the package file to be downloaded first (*order* 1).

For mobile users, you can decrease the connection time of the mobile device by using the **regex** keyword. When the browser connects to the security appliance, it includes the User-Agent string in the HTTP header. When the security appliance receives the string, if the string matches an expression configured for an image, it immediately downloads that image without testing the other client images.

The security appliance expands both SSL VPN client and Cisco Secure Desktop (CSD) package files in cache memory. In order for the security appliance to successfully expand the package files, there must be enough cache memory to store the images and files of the package file.

If the security appliance detects there is not enough cache memory to expand a package, it displays an error message to the console. The following example shows an error message reported after an attempt to install a package file with the **svc image** command:

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0.0070-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

If this occurs when you attempt to install an package file, examine the amount of cache memory remaining and the size of any previously installed packages with the **dir cache:/** command from global configuration mode. Adjust the cache size limit accordingly with the **cache-fs limit** command from webvpn configuration mode.

Examples

In the following example, the output of the **show webvpn svc** command indicates that the windows.pkg file has an order number of 1, and the windows2.pkg file has an order number of 15. When a remote computer establishes a connection, the windows.pkg file downloads first. If the file does not match the operating system, the windows2.pkg file downloads:

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 15
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

The user then reorders the package files using the **svc image** command, with the windows2.pkg file as the first file downloaded to the remote PC, and the windows.pkg file downloaded second:

```
hostname(config-webvpn)# svc image windows2.pkg 10
hostname(config-webvpn)# svc image windows.pkg 20
```

Reentering the **show webvpn svc** command shows the new order of the files.

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 10
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 20
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

The following example indicates the CSD image (located in sdesktop) and the SSL VPN client image (located in stc) use approximately 5.44 MB of cache memory. To create enough cache memore, the user sets the cache size limit to 6 MB:

```
hostname(config-webvpn)# dir cache:

Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)

hostname(config-webvpn)# cache-fs limit 6
hostname(config-webvpn)#
```

Related Commands

Command	Description
cache-fs limit	Limits the size of cache memory.
dir cache:	Displays the contents of cache memory.
show webvpn svc	Displays information about SSL VPN clients installed on the security appliance and loaded in cache memory for downloading to remote PCs.
svc enable	Enables the security appliance to download the client to remote computers.

svc keepalive

To configure the frequency of keepalive messages which a remote client sends to the security appliance over SSL VPN connections, use the **svc keepalive** command from group policy webvpn or username webvpn configuration modes.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc keepalive {**none** | *seconds*}

no svc keepalive {**none** | *seconds*}

Syntax Description

none	Disables keepalive messages.
seconds	Enables keepalive messages and specifies the frequency of the messages, from 15 to 600 seconds.

Defaults

The default is 20 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(3)	The default setting changed from disabled to 20 seconds.

Usage Guidelines

Both the legacy Cisco SSL VPN Client (SVC) and the Cisco AnyConnect VPN Client can send keepalive messages when they establish SSL VPN connections to the security appliance.

You can adjust the frequency of keepalive messages (specified by *seconds*), to ensure that an SSL VPN connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

Adjusting the frequency also ensures that the client does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

Note Keepalives are enabled by default. If you disable keepalives, in the event of a failover event, SSL VPN client sessions are not carried over to the standby device.

Examples

In the following example, the user configures the security appliance to enable the client to send keepalive messages, with a frequency of 300 seconds (5 minutes), for the existing group policy named *sales*:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

Related Commands

Command	Description
svc	Enables or requires an SSL VPN client for a specific group or user.
svc dpd-interval	Enables Dead Peer Detection (DPD) on the security appliance, and sets the frequency that either the client or the security appliance performs DPD.
svc keep-installer	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections.
svc rekey	Enables the client to perform a rekey on a session.

svc keep-installer

To enable the permanent installation of an SSL VPN client on a remote PC, use the **svc keep-installer** command from group-policy webvpn or username webvpn configuration modes.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

Syntax Description

installed	Disables the automatic uninstalling feature of the client. The client remains installed on the remote PC for future connections..
none	Specifies that the client uninstalls from the remote computer after the active connection terminates.

Defaults

The default is permanent installation of the client is enabled. The client remains on the remote computer at the end of the session.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

In the following example, the user enters group policy webvpn configuration mode and configures the group policy to remove the client at the end of the session:

```
hostname(config-group-policy)#webvpn
hostname(config-group-webvpn)# svc keep-installer none
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
show webvpn svc	Displays information about SSL VPN clients installed on the security appliance and loaded in cache memory for downloading to remote PCs.
svc	Enables or requires the client for a specific group or user.

svc enable	Enables the security appliance to download client files to remote PCs.
svc image	Specifies a client package file that the security appliance expands in cache memory for downloading to remote PCs.

svc modules

To specify the names of optional modules that the AnyConnect SSL VPN Client requires for optional features, use the **svc modules** command from group policy webvpn or username webvpn configuration mode.

To remove the command from the configuration, use the **no** form of the command:

svc modules {**none** | **value** *string*}

no svc modules {**none** | **value** *string*}

Syntax Description

string	The name of the optional module, up to 256 characters. Separate multiple strings with commas.

Defaults

The default is none. The security appliance does not download optional modules.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

To minimize download time, the client only requests downloads (from the security appliance) of modules that it needs for each feature that it supports. The **svc modules** command enables the security appliance to download these modules. If you choose **none**, the security appliance downloads the essential files with no optional modules.

Enable the Start Before Logon (SBL) feature using the *vpngina* string. This string enables the security appliance to download a graphical identification and authentication (GINA) for the AnyConnect client VPN connection.

For a list of values to enter for all client features, see the release notes for the Cisco AnyConnect VPN Client.

Examples

In the following example, the user enters group-policy attributes mode for the group policy *telecommuters*, enters webvpn configuration mode for the group policy, and specifies the string *vpngina*:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostame(config-group-webvpn)# svc modules value vpngina
```

Related Commands

Command	Description
show webvpn svc	Displays information about SSL VPN clients that are loaded in cache memory on the security appliance and available for download.
svc enable	Enables an SSL VPN client for a specific group or user.
svc image	Specifies a SSL VPN client package file that the security appliance expands in cache memory for downloading to remote PCs.

svc mtu

To adjust the MTU size for SSL VPN connections established by the Cisco AnyConnect VPN Client, use the **svc mtu** command from group policy webvpn or username webvpn configuration mode.

To remove the command from the configuration, use the **no** form of the command:

svc mtu *size*

no svc mtu *size*

Syntax Description

size	The MTU size in bytes, from 256 to 1406 bytes.

Defaults

The default size is 1406.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command affects only the AnyConnect client. The Cisco SSL VPN Client (SVC) is not capable of adjusting to different MTU sizes.

The default for this command in the default group policy is **no svc mtu**. The MTU size is adjusted automatically based on the MTU of the interface that the connection uses, minus the IP/UDP/DTLS overhead.

This command affects AnyConnect client connections established in only SSL and those established in SSL with DTLS.

Examples

The following example configures the MTU size to 500 bytes for the group policy *telecommuters*:

```
hostname(config)# group-policy telecommuters attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc mtu 500
```

Related Commands

Command	Description
svc keep-installer	Disables the automatic uninstalling feature of the client. After the initial download, the client remains on the remote PC after the connection terminates.
svc dtls	Enables DTLS for clients establishing SSL VPN connections.
show run webvpn	Displays configuration information about WebVPN, including **svc** commands.

svc profiles (group-policy or username attributes)

To specify a profiles package downloaded to Cisco AnyConnect VPN Client users, use the **svc profile** command from group policy webvpn or username attributes webvpn configuration mode.

To remove the command from the configuration and cause the value it to be inherited, use the **no** form of the command:

svc profiles {**value** *profile* | **none**}

no svc profiles {**value** *profile* | **none**}

Syntax Description

profile	The name of the profile.

Defaults

The default is none. The security appliance does not download profiles.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command, entered from group policy webvpn or username attributes webvpn configuration mode, enables the security appliance to download profiles to users on a group policy or username basis. To download a profile to *all* users, use this command from webvpn configuration mode.

A profile is a group of configuration parameters that the client uses to configure the connection entries that appear in the client user interface, including the names and addresses of host computers. You can create and save profiles using the AnyConnect user interface. You can also edit this file with a text editor and set advanced parameters that are not available through the user interface.

The client installation contains one profile template (AnyConnectProfile.tmpl) that you can edit and use as a basis to create other profile files. For more information about editing profiles, see the *Cisco AnyConnect VPN Client Administrator Guide*.

Examples

In the following example, the user queries the **svc profiles value** command, which displays the available profiles:

```
asa1(config-group-webvpn)# svc profiles value ?
```

```
config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

Then the user configures the group policy to use the profile *sales*:

```
asa1(config-group-webvpn)# svc profiles sales
```

Related Commands

Command	Description
show webvpn svc	Displays information about installed SSL VPN clients.
svc	Enables or requires an SSL VPN client for a specific group or user.
svc image	Specifies a client package file that the security appliance expands in cache memory for downloading to remote PCs.

svc profiles (webvpn)

To specify a file as a profiles package that the security appliance loads in cache memory and makes available to group policies and username attributes of Cisco AnyConnect VPN Client users, use the **svc profile** command from webvpn configuration mode.

To remove the command from the configuration and cause the security appliance to unload the package file from cache memory, use the **no** form of the command:

svc profiles {*profile path*}

no svc profiles {*profile path*}

Syntax Description

path	The path and filename of the profile file in flash memory of the security appliance.
profile	The name of the profile to create in cache.

Defaults

The default is none. The security appliance does not load a profiles package in cache memory.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A profile is a group of configuration parameters that the AnyConnect client uses to configure the connection entries that appear in the user interface, including the names and addresses of host computers. You can create and save profiles using the client user interface.

You can also edit this file with a text editor and set advanced parameters that are not available through the user interface. The client installation contains one profile template (AnyConnectProfile.tmpl) that you can edit and use as a basis to create other profile files. For more information about editing profiles, see the *Cisco AnyConnect VPN Client Administrator Guide.*

After you create a new profile and upload it to flash memory, identify the XML file to the security appliance as a profile using the **svc profiles** command in webvpn configuration mode. The command loads the files in cache memory on the security appliance. Then you can specify the profile for a group or user with the **svc profiles** command from group policy webvpn configuation or username attributes configuration mode.

Examples

In the following example, the user previously created two new profile files (sales_hosts.xml and engineering_hosts.xml) from the AnyConnectProfile.tmpl file provided in the client installation and uploaded them to flash memory of the security appliance.

Now the user identifies these files to the security appliance as AnyConnect profiles, specifying the names *sales* and *engineering*:

```
asa1(config-webvpn)# svc profiles sales disk0:sales_hosts.xml
asa1(config-webvpn)# svc profiles engineering disk0:engineering_hosts.xml
```

Entering the **dir cache:stc/profiles** command shows the profiles loaded into cache memory:

```
asa1(config-webvpn)# dir cache:stc/profiles

Directory of cache:stc/profiles/

0      ----  774         11:54:41 Nov 22 2006  engineering.pkg
0      ----  774         11:54:29 Nov 22 2006  sales.pkg

2428928 bytes total (18219008 bytes free)
asa1(config-webvpn)#
```

Now they are available to the **svc profiles** command in group policy webvpn configuration or username attributes configurate modes:

```
asa1(config)# group-policy sales attributes
asa1(config-group-policy)# webvpn
asa1(config-group-webvpn)# svc profiles value ?

config-group-webvpn mode commands/options:
Available configured profile packages:
  engineering
  sales
```

Related Commands

Command	Description
show webvpn svc	Displays information about installed SSL VPN clients.
svc	Enables or requires the SSL VPN client for a specific group or user.
svc image	Specifies an SSL VPN package file that the security appliance expands in cache memory for downloading to remote PCs.

svc rekey

To enable a remote client to perform a rekey on an SSL VPN connection, use the **svc rekey** command from group-policy webvpn or username webvpn configuration mode.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

Syntax Description

method ssl	Specifies that SSL renegotiation takes place during rekey.
method new-tunnel	Specifies that the client establishes a new tunnel during rekey.
time *minutes*	Specifies the number of minutes from the start of the session until the re-key takes place, from 4 to 10080 (1 week).
method none	Disables rekey.

Defaults

The default is none (disabled).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group policy webvpn configuration	•	—	•	—	—
username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Both the legac Cisco SSL VPN Client (SVC) and the Cisco AnyConnect VPN Client can perform a rekey on an SSL VPN connection to the security appliance.

We recommend that you configure SSL as the rekey method.

Examples

In the following example, the user specifies that remote clients belonging to the group policy *sales* renegotiate with SSL during rekey and rekey occurs 30 minutes after the session begins:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc rekey method ssl
hostname(config-group-webvpn)# svc rekey time 30
```

Related Commands

Command	Description
svc	Enables or requires the AnyConnect client for a specific group or user.
svc dpd-interval	Enables Dead Peer Detection (DPD) on the security appliance, and sets the frequency that either the AnyConnect client or the security appliance performs DPD.
svc keepalive	Specifies the frequency at which an AnyConnect client on a remote computer sends keepalive messages to the security appliance.
svc keep-installer	Enables the permanent installation of an AnyConnect client onto a remote computer.

switchport access vlan

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport access vlan** command in interface configuration mode to assign a switch port to a VLAN.

switchport access vlan *number*

no switchport access vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID to which you want to assign this switch port. The VLAN ID is between 1 and 4090.

Defaults

By default, all switch ports are assigned to VLAN 1.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In transparent firewall mode, you can configure two active VLANs in the ASA 5505 adaptive security appliance Base license and three active VLANs in the Security Plus license, one of which must be for failover.

In routed mode, you can configure up to three active VLANs in the ASA 5505 adaptive security appliance Base license, and up to 20 active VLANs with the Security Plus license.

An active VLAN is a VLAN with a **nameif** command configured.

You can assign one or more physical interfaces to each VLAN using the **switchport access vlan** command. By default, the VLAN mode of the interface is to be an access port (one VLAN associated with the interface). If you want to create a trunk port to pass multiple VLANs on the interface, use the **switchport mode access trunk** command to change the mode to trunk mode, and then use the **switchport trunk allowed vlan** command.

Examples

The following example assigns five physical interfaces to three VLAN interfaces:

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport mode

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport mode** command in interface configuration mode to set the VLAN mode to either access (the default) or trunk.

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

Syntax Description

access	Sets the switch port to access mode, which allows the switch port to pass traffic for only one VLAN. Packets exit the switch port without an 802.1Q VLAN tag. If a packet enters the switch port with a tag, the packet is dropped.
trunk	Sets the switch port to trunk mode, so it can pass traffic for multiple VLANs. Packets exit the switch port with an 802.1Q VLAN tag. If a packet enters the switch port without a tag, the packet is dropped.

Defaults

By default, the mode is access.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
7.2(2)	You can now configure multiple trunk ports, rather than being limited to one trunk.

Usage Guidelines

By default, the VLAN mode of the switch port is to be an access port (one VLAN associated with the switch port). In access mode, assign a switch port to a VLAN using the **switchport access vlan** command. If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode, and then use the **switchport trunk allowed vlan** command to assign multiple VLANs to the trunk. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk allowed vlan** command, the switch port remains in "line protocol down" state and cannot participate in traffic forwarding. Trunk mode is available only with the Security Plus license.

The **switchport vlan access** command does not take effect unless the mode is set to access mode. The **switchport trunk allowed vlan** command does not take effect unless the mode is set to trunk mode.

Examples

The following example configures an access mode switch port assigned to VLAN 100, and a trunk mode switch port assigned to VLANs 200 and 300:

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200,300
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport monitor

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport monitor** command in interface configuration mode to enable SPAN, also known as switch port monitoring. The port for which you enter this command (called the destination port) receives a copy of every packet transmitted or received on the specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor traffic. You can specify multiple source ports by entering this command multiple times. You can only enable SPAN for one destination port. To disable monitoring of a source port, use the **no** form of this command.

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

Syntax Description

source_port	Specifies the port you want to monitor. You can specify any Ethernet port as well as the Internal-Data0/1 backplane port that passes traffic between VLAN interfaces. Because the Internal-Data0/1 port is a Gigabit Ethernet port, you might overload the Fast Ethernet destination port with traffic. Monitor the port Internal-Data0/1 with caution.
tx	(Optional) Specifies that only transmitted traffic is monitored.
rx	(Optional) Specifies that only received traffic is monitored.
both	(Optional) Specifies that both transmitted and received traffic is monitored. **both** is the default.

Defaults

The default type of traffic to monitor is **both**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If you do not enable SPAN, then attaching a sniffer to one of the switch ports only captures traffic to or from that port. To capture traffic to or from multiple ports, you need to enable SPAN and identify the ports you want to monitor.

Use caution while connecting a SPAN destination port to another switch, as it could result in network loops.

Examples

The following example configures the Ethernet 0/1 port as the destination port which monitors the Ethernet 0/0 and Ethernet 0/2 ports:

```
hostname(config)# interface ethernet 0/1
hostname(config-if)# switchport monitor ethernet 0/0
hostname(config-if)# switchport monitor ethernet 0/2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.

switchport protected

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport protected** command in interface configuration mode to prevent the switch port from communicating with other protected switch ports on the same VLAN. This feature provides extra security to the other switch ports on a VLAN if one switch port becomes compromised.

switchport protected

no switchport protected

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the interfaces are not protected.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Communication to and from unprotected ports is not restricted by this command.

Examples

The following example configures seven switch ports. The Ethernet 0/4, 0/5, and 0/6 are assigned to the DMZ network and are protected from each other.

```
hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/5
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/6
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport trunk

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport trunk** command in interface configuration mode to assign VLANs to the trunk port. Use the **no** form of the command to remove a VLAN from the trunk.

switchport trunk {allowed vlans *vlan_range* | **native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* | **native vlan** v*lan*}

Syntax Description

allowed vlans *vlan_range*	Identifies one or more VLANs that you can assign to the trunk port. The VLAN ID is between 1 and 4090. The *vlan_range* can be identified in one of the following ways: • A single number (n) • A range (n-x) Separate numbers and ranges by commas, for example: 5,7-10,13,45-100 You can enter spaces instead of commas, but the command is saved to the configuration with commas. You can include the native VLAN in this command, but it is not required; the native VLAN is passed whether it is included in this command or not.
native vlan *vlan*	Assigns a native VLAN to the trunk. Packets on the native VLAN are not modified when sent over the trunk. For example, if a port has VLANs 2, 3 and 4 assigned to it, and VLAN 2 is the native VLAN, then packets on VLAN 2 that egress the port are not modified with an 802.1Q header. Frames that ingress (enter) this port and have no 802.1Q header are put into VLAN 2. Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.

Defaults

By default, no VLANs are assigned to the trunk.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
7.2(2)	This command was modified to allow more than 3 VLANs per switch port. Also, you can now configure multiple trunk ports, instead of being limited to only one. This command also uses commas instead of spaces to separate VLAN IDs.
7.2(4)/8.0(4)	Native VLAN support was introduced with the **native vlan** keywords.

Usage Guidelines

If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode using the **switchport mode trunk** command, and then use the **switchport trunk** command to assign VLANs to the trunk. This switch port cannot pass traffic until you assign at least one VLAN to it. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk allowed vlan** command, the switch port remains in "line protocol down" state and cannot participate in traffic forwarding. Trunk mode is available only with the Security Plus license. The **switchport trunk** command does not take effect unless the mode is set to trunk mode using the **switchport mode trunk** command.

Note This command is not downgrade-compatible to Version 7.2(1); the commas separating the VLANs are not recognized in 7.2(1). If you downgrade, be sure to separate the VLANs with spaces, and do not exceed the 3 VLAN limit.

Examples

The following example configures seven VLAN interfaces, including the failover interface which is configured using the **failover lan** command. VLANs 200, 201, and 202 are trunked on Ethernet 0/1.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.

synack-data

To set the action for TCP SYNACK packets that contain data, use the **synack-data** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

synack-data {**allow** | **drop**}

no synack-data

Syntax Description

allow	Allows TCP SYNACK packets that contain data.
drop	Drops TCP SYNACK packets that contain data.

Defaults

The default action is to drop TCP SYNACK packets that contain data.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **synack-data**—In tcp-map configuration mode, you can enter the **synack-data** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the security appliance to allow TCP SYNACK packets that contain data:

```
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# synack-data allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

syn-data

To allow or drop SYN packets with data, use the **syn-data** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

Syntax Description

allow	Allows SYN packets that contain data.
drop	Drops SYN packets that contain data.

Defaults

Packets with SYN data are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **syn-data** command in tcp-map configuration mode to drop packets with data in SYN packets.

According to the TCP specification, TCP implementations are required to accept data contained in a SYN packet. Because this is a subtle and obscure point, some implementations may not handle this correctly. To avoid any vulnerabilities to insertion attacks involving incorrect end-system implementations, you may choose to drop packets with data in SYN packets.

Examples

The following example shows how to drop SYN packets with data on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
```

```
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

sysopt connection permit-vpn

For traffic that enters the security appliance through a VPN tunnel and is then decrypted, use the **sysopt connection permit-vpn** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. To disable this feature, use the **no** form of this command.

sysopt connection permit-vpn

no sysopt connection permit-vpn

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command is now enabled by default. Also, only interface access lists are bypassed; group policy or per-user access lists remain in force.
7.1(1)	This command was changed from **sysopt connection permit-ipsec**.

Usage Guidelines

By default, the security appliance allows VPN traffic to terminate on a security appliance interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an interface access list. By default, you also do not need an interface access list for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the security appliance performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.)

You can require an interface access list to apply to the local IP addresses by entering the **no sysopt connection permit-vpn** command. See the the **access-list** and **access-group** commands to create an access list and apply it to an interface. The access list applies to the local IP address, and not to the original client IP address used before the VPN packet was decrypted.

Examples

The following example requires decrypted VPN traffic to comply with interface access lists:

```
hostname(config)# no sysopt connection permit-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection preserve-vpn-flows

To preserve and resume stateful (TCP) tunneled IPsec LAN-to-LAN traffic within the timeout period after the tunnel drops and recovers, use the **sysopt connection preserve-vpn-flows** command. To disable this feature, use the **no** form of this command.

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout window, data continues flowing successfully because the security appliance still has access to the state information in the original flow.

This command supports only IPsec LAN-to-LAN tunnels, including Network Extension Mode. It does not support AnyConnect/SSL VPN or IPsec remote-access tunnels.

Examples

The following example specifies that the state information for the tunnel will be preserved and the tunneled IPsec LAN-to-LAN VPN traffic will resume after the tunnel drops and is reestablished within the timeout period:

```
hostname(config)# no sysopt connection preserve-vpn-flows
```

To see whether this feature is enabled, enter the show run all command for sysopt:

```
hostname(config)# show run all sysopt
```

A sample result follows. For illustrative purposes, in this and all following examples, the preserve-vpn-flows item is bolded:

```
no sysopt connection timewait
```

```
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

To reclassify existing VPN flows, use the **sysopt connection reclassify-vpn** command in global configuration mode. To disable this feature, use the **no** form of this command.

sysopt connection reclassify-vpn

no sysopt connection reclassify-vpn

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced

Usage Guidelines

When VPN tunnels come up, this command reclassifies existing VPN flows to make sure that flows that need encryption get torn down and recreated.

This command only applies for LAN-to-LAN and dynamic VPNs. This command has no effect on EZVPN or VPN client connections.

Examples

The following example enables VPN reclassification:

```
hostname(config)# sysopt connection reclassify-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-vpn	Permits any packets that come from an IPsec tunnel without checking any acess lists for interfaces.

Command	Description
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection tcpmss

To ensure that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size, use the **sysopt connection tcpmss** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

Syntax Description

bytes	Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting *bytes* to 0. For the **minimum** keyword, the *bytes* represent the smallest maximum value allowed.
minimum	Overrides the maximum segment size to be no less than *bytes*, between 48 and 65535 bytes. This feature is disabled by default (set to 0).

Defaults

The default maximum value is 1380 bytes. The minimum feature is disabled by default (set to 0).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Both the host and the server can set the maximum segment size when they first establish a connection. If either maximum exceeds the value you set with the **sysopt connection tcpmss** command, then the security appliance overrides the maximum and inserts the value you set. If either maximum is less than the value you set with the **sysopt connection tcpmss minimum** command, then the security appliance overrides the maximum and inserts the "minimum" value you set (the minimum value is actually the smallest maximum allowed). For example, if you set a maximum size of 1200 bytes and a minimum size of 400 bytes, when a host requests a maximum size of 1300 bytes, then the security appliance alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the security appliance alters the packet to request 400 bytes (the minimum).

The default of 1380 bytes allows room for header information so that the total packet size does not exceed 1500 bytes, which is the default MTU for Ethernet. See the following calculation:

1380 data + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 bytes

If the host or server does not request a maximum segment size, the security appliance assumes that the RFC 793 default value of 536 bytes is in effect.

If you set the maximum size to be greater than 1380, packets might become fragmented, depending on the MTU size (which is 1500 by default). Large numbers of fragments can impact the performance of the security appliance when it uses the Frag Guard feature. Setting the minimum size prevents the TCP server from sending many small TCP data packets to the client and impacting the performance of the server and the network.

Note Although not advised for normal use of this feature, if you encounter the syslog IPFRAG messages 209001 and 209002, you can raise the *bytes* value.

Examples

The following example sets the maximum size to 1200 and the minimum to 400:

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection timewait

To force each TCP connection to linger in a shortened TIME_WAIT state of at least 15 seconds after the final normal TCP close-down sequence, use the **sysopt connection timewait** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to use this feature if an end host application default TCP terminating sequence is a simultaneous close.

sysopt connection timewait

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The default behavior of the security appliance is to track the shutdown sequence and release the connection after two FINs and the ACK of the last FIN segment. This quick release heuristic enables the security appliance to sustain a high connection rate, based on the most common closing sequence, known as the normal close sequence. However, in a simultaneous close, both ends of the transaction initiate the closing sequence, as opposed to the normal close sequence where one end closes and the other end acknowledges prior to initiating its own closing sequence (see RFC 793). Thus, in a simultaneous close, the quick release forces one side of the connection to linger in the CLOSING state. Having many sockets in the CLOSING state can degrade the performance of an end host. For example, some WinSock mainframe clients are known to exhibit this behavior and degrade the performance of the mainframe server. Using the **sysopt connection timewait** command creates a window for the simultaneous close down sequence to complete.

Examples

The following example enables the timewait feature:

```
hostname(config)# sysopt connection timewait
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.

sysopt nodnsalias

To disable DNS inspection that alters the DNS A record address when you use the **alias** command, use the **sysopt nodnsalias** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to disable DNS application inspection if you want the **alias** command to perform only NAT, and DNS packet alteration is undesirable.

sysopt nodnsalias {**inbound** | **outbound**}

no sysopt nodnsalias {**inbound** | **outbound**}

Syntax Description

inbound	Disables DNS record alteration for packets from lower security interfaces to higher security interfaces specified by an **alias** command.
outbound	Disables DNS record alteration for packets from higher security interfaces specified by an **alias** command to lower security interfaces.

Defaults

This feature is disabled by default (DNS record address alteration is enabled).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **alias** command performs NAT and DNS A record address alteration. In some cases, you might want to disable the DNS record alteration.

Examples

The following example disables the DNS address alteration for inbound packets:

```
hostname(config)# sysopt nodnsalias inbound
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.

Command	Description
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt noproxyarp	Disables proxy ARP on an interface.

sysopt noproxyarp

To disable proxy ARP for NAT global addresses or VPN client addresses on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

Syntax Description

interface_name	The interface name for which you want to disable proxy ARP.

Defaults

Proxy ARP is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(3)	This command was extended to affect VPN proxy ARPs when the VPN client addresses overlap with an internal network.

Usage Guidelines

If you have a VPN client address pool that overlaps with an existing network, the security appliance by default sends proxy ARPs on all interfaces. If you have another interface that is on the same Layer 2 domain, it will see the ARP requests and will answer with the MAC address of its interface. The result of this is that the return traffic of the VPN clients towards the internal hosts will go to the wrong interface and will get dropped. In this case, you need to enter the **sysopt noproxyarp** command for the interface where you do not want proxy ARPs.

In rare circumstances, you might want to disable proxy ARP for NAT global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking “Who is this IP address?” The device owning the IP address replies, “I own that IP address; here is my MAC address.”

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The security appliance uses proxy ARP when you configure NAT and specify a global address that is on the same network as the security appliance interface. The only way traffic can reach the hosts is if the security appliance uses proxy ARP to claim that the security appliance MAC address is assigned to destination global addresses.

Examples

The following example disables proxy ARP on the inside interface:

```
hostname(config)# sysopt noproxyarp inside
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

sysopt radius ignore-secret

To ignore the authentication key in RADIUS accounting responses, use the **sysopt radius ignore-secret** command in global configuration mode. To disable this feature, use the **no** form of this command. You might need to ignore the key for compatibility with some RADIUS servers.

sysopt radius ignore-secret

no sysopt radius ignore-secret

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Some RADIUS servers fail to include the key in the authenticator hash within the accounting acknowledgment response. This usage caveat can cause the security appliance to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in these acknowledgments, thus avoiding the retransmit problem. (The key identified here is the same one you set with the **aaa-server host** command.)

Examples

The following example ignores the authentication key in accounting responses:

```
hostname(config)# sysopt radius ignore-secret
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

CHAPTER 32

tcp-map through type echo Commands

tcp-map

To define a set of TCP normalization actions, use the **tcp-map** command in global configuration mode. The TCP normalization feature lets you specify criteria that identify abnormal packets, which the security appliance drops when they are detected. To remove the TCP map, use the **no** form of this command.

tcp-map *map_name*

no tcp-map *map_name*

Syntax Description

map_name	Specifies the TCP map name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This feature uses Modular Policy Framework. First define the TCP normalization actions you want to take using the **tcp-map** command. The **tcp-map** command enters tcp-map configuration mode, where you can enter one or more commands to define the TCP normalization actions. Then define the traffic to which you want to apply the TCP map using the **class-map** command. Enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, enter the **set connection advanced-options** command to reference the TCP map. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

The following commands are available in tcp-map configuration mode:

check-retransmission	Enables and disables the retransmit data checks.
checksum-verification	Enables and disable checksum verification.
exceed-mss	Allows or drops packets that exceed MSS set by peer.
queue-limit	Configures the maximum number of out-of-order packets that can be queued for a TCP connection. This command is only available on the ASA 5500 series adaptive security appliance. On the PIX 500 series security appliance, the queue limit is 3 and cannot be changed.

reserved-bits	Sets the reserved flags policy in the security appliance.
syn-data	Allows or drops SYN packets with data.
tcp-options	Allows or clears the selective-ack, timestamps, or window-scale TCP options.
ttl-evasion-protection	Enables or disables the TTL evasion protection offered by the security appliance.
urgent-flag	Allows or clears the URG pointer through the security appliance.
window-variation	Drops a connection that has changed its window size unexpectedly.

Examples

For example, to allow urgent flag and urgent offset packets for all traffic sent to the range of TCP ports between the well known FTP data port and the Telnet port, enter the following commands:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow

hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet

hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap

hostname(config-pmap-c)# service-policy pmap global
```

Related Commands

Command	Description
class (policy-map)	Specifies a class map to use for traffic classification.
clear configure tcp-map	Clears the TCP map configuration.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config tcp-map	Displays the information about the TCP map configuration.
tcp-options	Allows or clears the selective-ack, timestamps, or window-scale TCP options.

tcp-options

To allow or clear the TCP options through the security appliance, use the **tcp-options** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

no tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

tcp-options range *lower upper* {**allow** | **clear** | **drop**}

no tcp-options range *lower upper* {**allow** | **clear** | **drop**}

Syntax Description

allow	Allows the TCP options through the TCP normalizer.
clear	Clears the TCP options through the TCP normalizer and allows the packet.
drop	Drops the packet.
lower	Lower bound ranges (6-7) and (9-255).
selective-ack	Sets the selective acknowledgement mechanism (SACK) option. The default is to allow the SACK option.
timestamp	Sets the timestamp option. Clearing the timestamp option will disable PAWS and RTT. The default is to allow the timestamp option.
upper	Upper bound range (6-7) and (9-255).
window-scale	Sets the window scale mechanism option. The default is to allow the window scale mechanism option.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **tcp-options** command in tcp-map configuration mode to clear selective-acknowledgement, window-scale, and timestamp TCP options. You can also clear or drop packets with options that are not very well defined.

Examples

The following example shows how to drop all packets with TCP options in the ranges of 6-7 and 9-255:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# tcp-options range 6 7 drop
hostname(config-tcp-map)# tcp-options range 9 255 drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

telnet

To add Telnet access to the console and set the idle timeout, use the **telnet** command in global configuration mode. To remove Telnet access from a previously set IP address, use the **no** form of this command.

telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

no telnet {{*hostname* | *IP_address mask interface_name***} | {***IPv6_address interface_name***} | {timeout** *number*}**}**

Syntax Description

hostname	Specifies the name of a host that can access the Telnet console of the security appliance.
interface_name	Specifies the name of the network interface to Telnet to.
IP_address	Specifies the IP address of a host or network authorized to log in to the security appliance.
IPv6_address	Specifies the IPv6 address/prefix authorized to log in to the security appliance.
mask	Specifies the netmask associated with the IP address.
timeout *number*	Number of minutes that a Telnet session can be idle before being closed by the security appliance; valid values are from 1 to 1440 minutes.

Defaults

By default, Telnet sessions left idle for five minutes are closed by the security appliance.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	The variable *IPv6_address* was added. The **no telnet timeout** command was added too.

Usage Guidelines

The **telnet** command lets you specify which hosts can access the security appliance console with Telnet. You can enable Telnet to the security appliance on all interfaces. However, the security appliance enforces that all Telnet traffic to the outside interface be protected by IPSec. To enable a Telnet session to the outside interface, configure IPSec on the outside interface to include IP traffic that is generated by the security appliance and enable Telnet on the outside interface.

Use the **no telnet** command to remove Telnet access from a previously set IP address. Use the **telnet timeout** command to set the maximum time that a console Telnet session can be idle before being logged off by the security appliance. You cannot use the **no telnet** command with the **telnet timeout** command.

If you enter an IP address, you must also enter a netmask. There is no default netmask. Do not use the subnetwork mask of the internal network. The *netmask* is only a bit mask for the IP address. To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255.

If IPSec is operating, you can specify an unsecure interface name, which is typically, the outside interface. At a minimum, you might configure the **crypto map** command to specify an interface name with the **telnet** command.

Use the **passwd** command to set a password for Telnet access to the console. The default is **cisco**. Use the **who** command to view which IP addresses are currently accessing the security appliance console. Use the **kill** command to terminate an active Telnet console session.

If you use the **aaa** command with the **console** keyword, Telnet console access must be authenticated with an authentication server.

Note If you have configured the **aaa** command to require authentication for security appliance Telnet console access and the console login request times out, you can gain access to the security appliance from the serial console by entering the security appliance username and the password that was set with the **enable password** command.

Examples

This example shows how to permit hosts 192.168.1.3 and 192.168.1.4 to access the security appliance console through Telnet. In addition, all the hosts on the 192.168.2.0 network are given access.

```
hostname(config)# telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# telnet 192.168.1.4 255.255.255.255 inside
hostname(config)# telnet 192.168.2.0 255.255.255.0 inside
hostname(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

This example shows how to change the maximum session idle duration:

```
hostname(config)# telnet timeout 10
hostname(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

This example shows a Telnet console login session (the password does not display when entered):

```
hostname# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
hostname>
```

You can remove individual entries with the **no telnet** command or all telnet command statements with the **clear configure telnet** command:

```
hostname(config)# no telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

```
hostname(config)# clear configure telnet
```

Related Commands

Command	Description
clear configure telnet	Removes a Telnet connection from the configuration.
kill	Terminates a Telnet session.
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the security appliance.
who	Displays active Telnet administration sessions on the security appliance.

terminal

To allow system log messages to show in the current Telnet session, use the **terminal monitor** command in privileged EXEC mode. To disable system log messages, use the **terminal no monitor** command.

terminal {**monitor** | **no monitor**}

Syntax Description

monitor	Enables the display of system log messages in the current Telnet session.
no monitor	Disables the display of system log messages in the current Telnet session.

Defaults

System log messages are disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to display system log messages and disable system log messages in the current session:

```
hostname# terminal monitor
hostname# terminal no monitor
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the "`---more---`" prompt. This command is saved to the configuration.
show running-config terminal	Displays the current terminal settings.
terminal pager	Sets the number of lines to display in a Telnet session before the "`---more---`" prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

terminal pager

To set the number of lines on a page before the "---more---" prompt appears for Telnet sessions, use the **terminal pager** command in privileged EXEC mode.

terminal pager [lines] *lines*

Syntax Description

[**lines**] *lines*	Sets the number of lines on a page before the "---more---" prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Defaults

The default is 24 lines.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command changes the pager line setting only for the current Telnet session. To save a new default pager setting to the configuration, use the **pager** command.

If you Telnet to the admin context, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

Examples

The following example changes the number of lines displayed to 20:

```
hostname# terminal pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is saved to the configuration.

Command	Description
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messsages to display on the Telnet session.
terminal width	Sets the terminal display width in global configuration mode.

terminal width

To set the width for displaying information during console sessions, use the **terminal width** command in global configuration mode. To disable, use the **no** form of this command.

terminal width *columns*

no terminal width *columns*

Syntax Description

columns	Specifies the terminal width in columns. The default is 80. The range is 40 to 511.

Defaults

The default display width is 80 columns.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to terminal display width to 100 columns:

```
hostname# terminal width 100
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Sets the terminal line parameters in privileged EXEC mode.

test aaa-server

To check whether the security appliance can authenticate or authorize users with a particular AAA server, use the **test aaa-server** command in privileged EXEC mode. Failure to reach the AAA server may be due to incorrect configuration on the security appliance, or the AAA server may be unreachable for other reasons, such as restrictive network configurations or server downtime.

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*]}

Syntax Description

authentication	Tests a AAA server for authentication capability.
authorization	Tests a AAA server for legacy VPN authorization capability.
host *ip_address*	Specifies the server IP address. If you do not specify the IP address in the command, you are prompted for it.
password *password*	Specifies the user password. If you do not specify the password in the command, you are prompted for it.
server_tag	Specifies the AAA server tag as set by the **aaa-server** command.
username *username*	Specifies the username of the account used to test the AAA server settings. Make sure the username exists on the AAA server; otherwise, the test will fail. If you do not specify the username in the command, you are prompted for it.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **test aaa-server** command lets you verify that the security appliance can authenticate users with a particular AAA server, and for legacy VPN authorization, if you can authorize a user. This command lets you test the AAA server without having an actual user who attempts to authenticate or authorize. It also helps you isolate whether AAA failures are due to misconfiguration of AAA server parameters, a connection problem to the AAA server, or other configuration errors on the security appliance.

Examples

The following example configures a RADIUS AAA server named srvgrp1 on host 192.168.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650. The **test aaa-server** command following the setup of the AAA server parameters indicates that the authentication test failed to reach the server.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

The following is sample output from the **test aaa-server** command with a successful outcome:

```
hostname# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

Related Commands

Command	Description
aaa authentication console	Configures authentication for management traffic.
aaa authentication match	Configures authentication for through traffic.
aaa-server	Creates a AAA server group.
aaa-server host	Adds a AAA server to a server group.

test dynamic-access-policy attributes

To enter the dap attributes mode, from Privileged EXEC mode, enter the **test dynamic-access-policy attributes** command. Doing so lets you specify user and endpoint attribute value pairs.

dynamic-access-policy attributes

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Normally the security appliance retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The security appliance writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record.

This feature lets you experiment with creating a DAP record.

Examples

The following example shows how to use the **attributes** command.

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
attributes	Enters attributes mode, in which you can specify user attribute value pairs.
display	Displays current attribute list.

test dynamic-access-policy execute

test regex

To test a regular expression, use the **test regex** command in privileged EXEC mode.

test regex *input_text regular_expression*

Syntax Description

input_text	Specifies the text that you want to match with the regular expression.
regular_expression	Specifies the regular expression up to 100 characters in length. See the **regex** command for a list of metacharacters you can use in the regular expression.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **test regex** command tests a regular expression to make sure it matches what you think it will match.

If the regular expression matches the input text, you see the following message:

```
INFO: Regular expression match succeeded.
```

If the regular expression does not match the input text, you see the following message:

```
INFO: Regular expression match failed.
```

Examples

The following example tests input text against a regular expression:

```
hostname# test regex farscape scape
INFO: Regular expression match succeeded.

hostname# test regex farscape scaper

INFO: Regular expression match failed.
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
class-map type regex	Creates a regular expression class map.
regex	Creates a regular expression.

test sso-server

To test an SSO server with a trial authentication request, use the **test sso-server** command in privileged EXEC mode.

test sso-server *server-name* **username** *user-name*

Syntax Description

server-name	Specifies the name of the SSO server being tested.
user-name	Specifies the name of a user on the SSO server being tested.

Defaults

No default values or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn	•	—	•	—	—
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
Global configuration mode	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **test sso-server** command tests whether an SSO server is recognized and responding to authentication requests.

If the SSO server specified by the *server-name* argument is not found, the following error appears:

```
ERROR: sso-server server-name does not exist
```

If the SSO server is found but the user specified by the *user-name* argument is not found, the authentication is rejected.

In the authentication, the security appliance acts as a proxy for the WebVPN user to the SSO server. The security appliance currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. This command applies to both types of SSO Servers.

Examples

The following example, entered in privileged EXEC mode, successfully tests an SSO server named my-sso-server using a username of Anyuser:

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
hostname#
```

The following example shows a test of the same server, but the user, Anotheruser, is not recognized and the authentication fails:

```
hostname# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
hostname#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

text-color

To set a color for text in the WebVPN title bar on the login, home page, and file access page, use the **text-color** command in webvpn mode. To remove a text color from the configuration and reset the default, use the no form of this command.

text-color [*black* | *white* | *auto***]**

no text-color

Syntax Description

auto	Chooses black or white based on the settings for the secondary-color command. That is, if the secondary color is black, this value is white.
black	The default text color for title bars is white.
white	You can change the color to black.

Defaults

The default text color for the title bars is white.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set the text color for title bars to black:

```
hostname(config)# webvpn
hostname(config-webvpn)# text-color black
```

Related Commands

Command	Description
secondary-text-color	Sets the secondary text color for the WebVPN login, home page, and file access page.

tftp-server

To specify the default TFTP server and path and filename for use with **configure net** or **write net** commands, use the **tftp-server** command in global configuration mode. To remove the server configuration, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

Syntax Description

interface_name	Specifies the gateway interface name. If you specify an interface other than the highest security interface, a warning message informs you that the interface is unsecure.
server	Sets the TFTP server IP address or name. You can enter an IPv4 or IPv6 address.
filename	Specifies the path and filename.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	The gateway interface is now required.

Usage Guidelines

The **tftp-server** command simplifies entering the **configure net** and **write net** commands. When you enter the **configure net** or **write net** commands, you can either inherit the TFTP server specified by the **tftp-server** command, or provide your own value. You can also inherit the path in the **tftp-server** command as is, add a path and filename to the end of the **tftp-server** command value, or override the **tftp-server** command value.

The security appliance supports only one **tftp-server** command.

Examples

This example shows how to specify a TFTP server and then read the configuration from the /temp/config/test_config directory:

```
hostname(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
hostname(config)# configure net
```

Related Commands

Command	Description
configure net	Loads the configuration from the TFTP server and path you specify.
show running-config tftp-server	Displays the default TFTP server address and the directory of the configuration file.

tftp-server address

To specify the TFTP servers in the cluster, use the **tftp-server address** command in phone-proxy configuration mode. To remove the TFTP server from the Phone Proxy configuration, use the **no** form of this command.

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

Syntax Description

ip_address	Specifies the address of the TFTP server.
interface *interface*	Specifies the interface on which the TFTP server resides. This must be the real address of the TFTP server.
port	(Optional) This is the port the TFTP server is listening in on for the TFTP requests. This should be configured if it is not the default TFTP port 69.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The Phone Proxy must have at least one CUCM TFTP server configured. Up to five TFTP servers can be configured for the Phone Proxy.

The TFTP server is assumed to be behind the firewall on the trusted network; therefore, the Phone Proxy intercepts the requests between the IP phones and TFTP server. The TFTP server must reside on the same interface as the CUCM.

Create the TFTP server using the internal IP address and specify the interface on which the TFTP server resides.

On the IP phones, the IP address of the TFTP server must be configured as follows:

- If NAT is configured for the TFTP server, use the TFTP server's global IP address.
- If NAT is not configured for the TFTP server, use the TFTP server's internal IP address.

If the service-policy is applied globally, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on all ingress interfaces, except for the interface on which the TFTP server resides. When the service-policy is applied on a specific interface, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on that specified interface to the phone-proxy module.

If a NAT rule is configured for the TFTP server, it must be configured prior to applying the service-policy so that the global address of the TFTP server is used when installing the classification rule.

Examples

The following example shows the use of the **tftp-server address** command to configure two TFTP servers for the Phone Proxy:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

threat-detection basic-threat

To enable basic threat detection, use the **threat-detection basic-threat** command in global configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection basic-threat

no threat-detection basic-threat

Syntax Description

This command has no arguments or keywords.

Defaults

Basic threat detection is enabled by default. The following default rate limits are used:

Table 32-1 Basic Threat Detection Default Settings

	Trigger Settings	
Packet Drop Reason	**Average Rate**	**Burst Rate**
• DoS attack detected • Bad packet format • Connection limits exceeded • Suspicious ICMP packets detected	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 10 second period.
	80 drops/sec over the last 3600 seconds.	320 drops/sec over the last 60 second period.
Scanning attack detected	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
	4 drops/sec over the last 3600 seconds.	8 drops/sec over the last 60 second period.
Incomplete session detected such as TCP SYN attack detected or no data UDP session attack detected (combined)	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 10 second period.
	80 drops/sec over the last 3600 seconds.	160 drops/sec over the last 60 second period.
Denial by access lists	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 10 second period.
	320 drops/sec over the last 3600 seconds.	640 drops/sec over the last 60 second period.
• Basic firewall checks failed • Packets failed application inspection	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 10 second period.
	320 drops/sec over the last 3600 seconds.	1280 drops/sec over the last 60 second period.
Interface overload	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 10 second period.
	1600 drops/sec over the last 3600 seconds.	6400 drops/sec over the last 60 second period.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

When you enable basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the following reasons:

- Denial by access lists
- Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length)
- Connection limits exceeded (both system-wide resource limits, and limits set in the configuration)
- DoS attack detected (such as an invalid SPI, Stateful Firewall check failure)
- Basic firewall checks failed (This option is a combined rate that includes all firewall-related packet drops in this bulleted list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.)
- Suspicious ICMP packets detected
- Packets failed application inspection
- Interface overload
- Scanning attack detected (This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.)
- Incomplete session detection such as TCP SYN attack detected or no data UDP session attack detected

When the security appliance detects a threat, it immediately sends a system log message (730100) and alerts ASDM.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 32-1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command. You can override the default settings for each type of event by using the **threat-detection rate** command.

If an event rate is exceeded, then the security appliance sends a system message. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst event rate is 1/60th of the average rate interval or 10 seconds, whichever is higher. For each event received, the security appliance checks the average and burst rate limits; if both rates are exceeded, then the security appliance sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can change the default rate limits for each event type using the **threat-detection rate** command in global configuration mode. If you enable scanning threat detection using the **threat-detection scanning-threat** command, then this command with the **scanning-threat** keyword also sets the when a host is considered to be an attacker or a target; otherwise the default **scanning-threat** value is used for both basic and scanning threat detection. To return to the default setting, use the **no** form of this command.

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

Syntax Description

acl-drop	Sets the rate limit for dropped packets caused by denial by access lists.
average-rate *av_rate*	Sets the average rate limit between 0 and 2147483647 in drops/sec.
bad-packet-drop	Sets the rate limit for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
burst-rate *burst_rate*	Sets the burst rate limit between 0 and 2147483647 in drops/sec. The burst rate is calculated as the average rate every *N* seconds, where *N* is the burst rate interval. The burst rate interval is 1/60th of the **rate-interval** *rate_interval* value or 10 seconds, whichever is larger.
conn-limit-drop	Sets the rate limit for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	Sets the rate limit for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	Sets the rate limit for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop**, **inspect-drop**, and **scanning-threat**.
icmp-drop	Sets the rate limit for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	Sets the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	Sets the rate limit for dropped packets caused by an interface overload.
rate-interval *rate_interval*	Sets the average rate interval between 600 seconds and 2592000 seconds (30 days). The rate interval is used to determine the length of time over which to average the drops. It also determines the burst threshold rate interval.

scanning-threat	Sets the rate limit for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	Sets the rate limit for dropped packets caused by an incomplete session, such as TCP SYN attack or no data UDP session attack.

Defaults

When you enable basic threat detection using the **threat-detection basic-threat** command, the following default rate limits are used:

Table 32-2 Basic Threat Detection Default Settings

	Trigger Settings	
Packet Drop Reason	**Average Rate**	**Burst Rate**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 10 second period.
	100 drops/sec over the last 3600 seconds.	400 drops/sec over the last 60 second period.
scanning-threat	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
	5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 60 second period.
syn-attack	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 10 second period.
	100 drops/sec over the last 3600 seconds.	200 drops/sec over the last 60 second period.
acl-drop	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 10 second period.
	400 drops/sec over the last 3600 seconds.	800 drops/sec over the last 60 second period.
• **fw-drop** • **inspect-drop**	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 10 second period.
	400 drops/sec over the last 3600 seconds.	1600 drops/sec over the last 60 second period.
interface-drop	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 10 second period.
	2000 drops/sec over the last 3600 seconds.	8000 drops/sec over the last 60 second period.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can configure up to three different rate intervals for each event type.

When you enable basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the event types described in the "Syntax Description" table.

When the security appliance detects a threat, it immediately sends a system log message (730100) and alerts ASDM.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 32-1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command.

If an event rate is exceeded, then the security appliance sends a system message. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event received, the security appliance checks the average and burst rate limits; if both rates are exceeded, then the security appliance sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection scanning-threat

To enable scanning threat detection, use the **threat-detection scanning-threat** command in global configuration mode. To disable scanning threat detection, use the **no** form of this command.

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

Syntax Description

duration *seconds*	Sets the duration of a shun for an attacking host, between 10 and 2592000 seconds. The default length is 3600 seconds (1 hour).
except	Exempts IP addresses from being shunned. Enter this command multiple times to identify multiple IP addresses or network object groups to exempt from shunning.
ip-address *ip_address mask*	Specifies the IP address you want to exempt from shunning.
object-group *network_object_group_id*	Specifies the network object group that you want to exempt from shunning. See the **object-group network** command to create the object group.
shun	Automatically terminates a host connection when the security appliance identifies the host as an attacker, in addition to sending system log message 730101.

Defaults

The default shun duration is 3600 seconds (1 hour).

The following default rate limits are used for scanning attack events:

Table 32-3 Default Rate Limits for Scanning Threat Detection

Average Rate	Burst Rate
5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 60 second period.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The **duration** keyword was added.

Usage Guidelines

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the security appliance scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

Caution The scanning threat detection feature can affect the security appliance performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

You can configure the security appliance to send system log messages about an attacker or you can automatically shun the host. By default, the system log message 730101 is generated when a host is identified as an attacker.

The security appliance identifies attackers and targets when the scanning threat event rate is exceeded. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event detected that is considered to be part of a scanning attack, the security appliance checks the average and burst rate limits. If either rate is exceeded for traffic sent from a host, then that host is considered to be an attacker. If either rate is exceeded for traffic received by a host, then that host is considered to be a target. You can change the rate limits for scanning threat events using the **threat-detection rate scanning-threat** command.

To view hosts categorized as attackers or as targets, use the **show threat-detection scanning-threat** command.

To view shunned hosts, use the **show threat-detection shun** command. To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following example enables scanning threat detection and automatically shuns hosts categorized as attackers, except for hosts on the 10.1.1.0 network. The default rate limits for scanning threat detection are also changed.

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

Related Commands

Command	Description
clear threat-detection shun	Releases a host from being shunned.
show threat-detection scanning-threat	Shows the hosts that are categorized as attackers and targets.

Command	Description
show threat-detection shun	Shows hosts that are currently shunned.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.

threat-detection statistics

To enable scanning threat detection statistics, use the **threat-detection statistics** command in global configuration mode. To disable scanning threat detection statistics, use the **no** form of this command.

Caution Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. The **threat-detection statistics host** command affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. The **threat-detection statistics port** command, however, has modest impact.

threat-detection statistics [**access-list** | **host** | **port** | **protocol | tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol | tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

Syntax Description

access-list	(Optional) Enables statistics for access list denies. Access list statistics are only displayed using the **show threat-detection top access-list** command.
average-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.
burst-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
host	(Optional) Enables host statistics. The host statistsics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
port	(Optional) Enables port statistics.
protocol	(Optional) Enables protocol statistics.
rate-interval *minutes*	(Optional) For TCP Intercept, sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the security appliance samples the number of attacks 60 times.
tcp-intercept	(Optional) Enables statistics for attacks intercepted by TCP Intercept. See the **set connection embryonic-conn-max command**, or the **nat** or **static** commands to enable TCP Intercept.

Defaults

Access list statistics are enabled by default. If you do not specify any options in this command, then you enable all options.

The default **tcp-intercept rate-interval** is 30 minutes. The default **burst-rate** is 400 per second. The default **average-rate** is 200 per second.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)	The **tcp-intercept** keyword was added.

Usage Guidelines

View statistics using the **show threat-detection statistics** commands.

You do not need to enable scanning threat detection using the **threat-detection scanning-threat** command; you can configure detection and statistics separately.

Examples

The following example enables scanning threat detection and scanning threat statistics for all types except host:

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection statistics access-list
hostname(config)# threat-detection statistics port
hostname(config)# threat-detection statistics protocol
hostname(config)# threat-detection statistics tcp-intercept
```

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

threshold

To set the threshold value for over threshold events in SLA monitoring operations, use the **threshold** command in SLA monitor configuration mode. To restore the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description

milliseconds	Specifies the number of milliseconds for a rising threshold to be declared. Valid values are from 0 to 2147483647. This value should not be larger than the value set for the timeout.

Defaults

The default threshold is 5000 milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The threshold value is only used to indicate over threshold events, which do not affect reachability but may be used to evaluate the proper settings for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time the SLA operation waits for a response.

timeout

To set the global maximum idle time duration for various features, use the **timeout** command in global configuration mode. To set all timeouts to the default, use the **no** form of this command. To reset a single feature to its default, reenter the **timeout** command with the default value.

timeout {**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

Syntax Description

absolute	(Optional) Requires a reauthentication after the uauth timeout expires. The **absolute** keyword is enabled by default. To set the uauth timer to timeout after a period of inactivity, enter the **inactivity** keyword instead.
conn	(Optional) Specifies the idle time after which a connection closes, between 0:05:0 and 1193:0:0. The default is 1 hour (1:0:0). Use **0** to never time out a connection.
hh:*mm*:*ss*	Specifies the timeout in hours, minutes, and seconds. Use **0** to never time out a connection, if available.
h225	(Optional) Specifies the idle time after which an H.225 signaling connection closes, between 0:0:0 and 1193:0:0. The default is 1 hour (1:0:0). A timeout value of 0:0:01 disables the timer and closes the TCP connection immediately after all calls are cleared.
h323	(Optional) Specifies the idle time after which H.245 (TCP) and H.323 (UDP) media connections close, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.
half-closed	(Optional) Specifies the idle time after which a TCP half-closed connection will be freed, between 0:5:0 and 1193:0:0. The default is 10 minutes (0:10:0). Use **0** to never time out a connection.
icmp	(Optional) Specifies the idle time for ICMP, between 0:0:02 and 1193:0:0 The default is 2 seconds (0:0:02).
inactivity	(Optional) Requires uauth reauthentication after the inactivity timeout expires.
mgcp	(Optional) Sets the idle time after which an MGCP media connection is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0)
mgcp-pat	(Optional) Sets the absolute interval after which an MGCP PAT translation is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0).
rpc	(Optional) Specifies the idle time until an RPC slot is freed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:05:0).
sip	(Optional) Specifies the dle time after which a SIP control connection will be closed, between 0:5:0 and 1193:0:0. The default is 30 minutes (0:30:0). Use **0** to never time out a connection.

sip-disconnect	(Optional) Specifies the idle time after which a SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 1193:0:0. The default is 2 minutes (0:2:0).
sip-invite	(Optional) Specifies the idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 1193:0:0. The default is 3 minutes (0:3:0).
sip_media	(Optional) Specifies the idle time after which a SIP media connection will be closed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use **0** to never time out a connection. The SIP media timer is used used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
sip-provisional-media	(Optional) Specifies timeout value for SIP provisional media connections, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).
sunrpc	(Optional) Specifies the idle time after which a SUNRPC slot will be closed, between 0:1:0 and 1193:0:0. The default is 10 minutes (0:10:0). Use **0** to never time out a connection.
uauth	(Optional) Specifies the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The default timer is absolute; you can set the timeout to occur after a period of inactivity by entering the **inactivity** keyword. The **uauth** duration must be shorter than the **xlate** duration. Set to **0** to disable caching. Do not use **0** if passive FTP is used for the connection or if the **virtual http** command is used for web authentication.
udp	(Optional) Specifies the idle time until a UDP slot is freed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use **0** to never time out a connection.
xlate	(Optional) Specifies the idle time until a translation slot is freed, between 0:1:0 and 1193:0:0. The default is 3 hours (3:0:0).

Defaults

The defaults are as follows:

- **conn** *hh*:*mm*:*ss* is 1 hour (**1:0:0**).
- **h225** *hh*:*mm*:*ss* is 1 hour (**1:0:0**).
- **h323** *hh*:*mm*:*ss* is 5 minutes (**0:5:0**).
- **half-closed** *hh*:*mm*:*ss* is 10 minutes (**0:10:0**).
- **icmp** *hh:mm:ss* is 2 seconds (**0:0:2**)
- **mgcp** *hh:mm:ss* is 5 minutes (**0:5:0**).
- **mgcp-pat** *hh:mm:ss* is 5 minutes (**0:5:0**).
- **rpc** *hh*:*mm*:*ss* is 5 minutes (**0:5:0**).
- **sip** *hh:mm:* is 30 minutes (**0:30:0**).
- **sip-disconnect** *hh:mm:ss* is 2 minutes (**0:2:0**).
- **sip-invite** *hh:mm:ss* is 3 minutes (**0:3:0**).
- **sip_media** *hh:mm:ss* is 2 minutes (**0:2:0**).

- **sip-provisional-media** *hh:mm:ss* is 2 minutes (**0:2:0**).
- **sunrpc** *hh:mm:ss* is 10 minutes (**0:10:0**)
- **uauth** *hh:mm:ss* is 5 minutes (**00:5:00**) **absolute**.
- **udp** *hh*:*mm*:*ss* is 2 minutes (**00:02:00**).
- **xlate** *hh*:*mm*:*ss* is 3 hours (**03:00:00**).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration mode	•	•	•	•	—

Command History

Release	Modification
7.2(1)	The **mgcp-pat**, **sip-disconnect**, and **sip-invite** keywords were added.
7.2(4)/8.0(4)	The **sip-provisional-media** keyword was added.

Usage Guidelines

The **timeout** command lets you set global timeouts. For some features, the **set connection timeout** command takes precedence for traffic identified in the command.

You can enter multiple keywords and values after the **timeout** command.

The connection timer (**conn**) takes precedence over the translation timer (**xlate**); the translation timer works only after all connections have timed out.

Examples

The following example shows how to configure the maximum idle time durations:

```
hostname(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
hostname(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

Related Commands

Command	Description
clear configure timeout	Clears the timeout configuration and resets it to the defaults.
set connection timeout	Sets connection timeouts using Modular Policy Framework.
show running-config timeout	Displays the timeout value of the designated protocol.

timeout (aaa-server host)

To configure the host-specific maximum response time, in seconds, allowed before giving up on establishing a connection with the AAA server, use the **timeout** command in aaa-server host mode. To remove the timeout value and reset the timeout to the default value of 10 seconds, use the **no** form of this command.

timeout *seconds*

no timeout

Syntax Description

seconds	Specifies the timeout interval (1-60 seconds) for the request. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server.

Defaults

The default timeout value is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server host configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid for all AAA server protocol types.

Use the **timeout** command to specify the length of time during which the security appliance attempts to make a connection to a AAA server. Use the **retry-interval** command to specify the amount of time the security appliance waits between connection attempts.

The timeout is the total amount of time that the security appliance spends trying to complete a transaction with a server. The retry interval determines how often the communication is retried during the timeout period. Thus, if the retry interval is greater than or equal to the timeout value, you will see no retries. If you want to see retries, the retry interval musts be less than thte timeout value.

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host 1.2.3.4 to use a timeout value of 30 seconds, with a retry interval of 10 seconds. Thus, the security appliance tries the communication attempt three times before giving up after 30 seconds.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 30
hostname(config-aaa-server-host)# retry-interval 10
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa server host configuration mode so you can configure AAA server parameters that are host specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa	Displays the current AAA configuration values.

timeout (dns-server-group configuration mode)

To specify the amount of time to wait before trying the next DNS server, use the **timeout** command in dns-server-group configuration mode. To restore the default timeout, use the **no** form of this command.

timeout *seconds*

no timeout [*seconds*]

Syntax Description

seconds	Specifies the timeout in seconds between 1 and 30. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles. Use the **retries** command in dns-server-group configuration mode to configure the number of retries.

Defaults

The default timeout is 2 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example sets the timeout to 1 second for the DNS server group “dnsgroup1”:

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns timeout 1
```

Related Commands

Command	Description
clear configure dns	Removes all user-created DNS server-groups and resets the default server group’s attributes to the default values.
domain-name	Sets the default domain name.
retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
show running-config dns server-group	Shows the current running DNS server-group configuration.

timeout (gtp-map)

To change the inactivity timers for a GTP session, use the **timeout** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to set these intervals to their default values.

timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

no timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

Syntax Description

hh:*mm*:*ss*	This is the timeout where *hh* specifies the hour, *mm* specifies the minutes, *ss* specifies the seconds, and a colon (:) separates these three components. The value 0 means never tear down immediately.
gsn	Specifies the period of inactivity after which a GSN will be removed.
pdp-context	Specifies the maximum period of time allowed before beginning to receive the PDP context.
request	Specifies the the maximum period of time allowed before beginning to receive the GTP message.
signaling	Specifies the period of inactivity after which the GTP signaling will be removed.
t3-response	Specifies the maximum wait time for a response before a GTP connection is removed.
tunnel	Specifies the period of inactivity after which the GTP tunnel will be torn down.

Defaults

The default is 30 minutes for **gsn**, **pdp-context**, and **signaling**.

The default for **request** is 1 minute.

The default for **tunnel** is 1 hour (in the case where a Delete PDP Context Request is not received).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The Packet Data Protocol (PDP) context is identified by the Tunnel Identifier (TID), which is a combination of IMSI and NSAPI. Each MS can have up to 15 NSAPIs, allowing it to create multiple PDP contexts each with a different NSAPI, based on application requirements for varied QoS levels.

A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station user.

Examples

The following example sets a timeout value for the request queue of 2 minutes:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# timeout request 00:02:00
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

timeout (radius-accounting)

To change the inactivity timers for RADIUS accounting users, use the **timeout** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command. Use the **no** form of this command to set these intervals to their default values.

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

Syntax Description

hh:*mm*:*ss*	This is the timeout where *hh* specifies the hour, *mm* specifies the minutes, *ss* specifies the seconds, and a colon (:) separates these three components. The value 0 means never tear down immediately. The default is one hour.
users	Specifies the timeout for users.

Defaults

The default timeout for users is one hour.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example sets a timeout value for the user of ten minutes:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout user 00:10:00
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

timeout (sla monitor)

To set the amount of time the SLA operation waits for a response to the request packets, use the **timeout** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

milliseconds	0 to 604800000.

Defaults

The default timeout value is 5000 milliseconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **frequency** command to set how often the SLA operation sends out the request packets and the **timeout** command to set how long the SLA operation waits to receive a response to those requests. The values specified for the **timeout** command cannot be greater than the value specified for the **frequency** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
sla monitor	Defines an SLA monitoring operation.

timeout pinhole

To configure the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes, use the **timeout pinhole** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

timeout pinhole *hh:mm:ss*

no timeout pinhole

Syntax Description

hh:mm:ss	The timeout for pinhole connections. Value is between 0:0:1 and 1193:0:0.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure the pinhole timeout for pin hole connections in a DCERPC inspection policy map:

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout pinhole 0:10:00
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

time-range

To enter time-range configuration mode and define a time range that you can attach to traffic rules, or an action, use the **time-range** command in global configuration mode. To disable, use the **no** form of this command.

time-range *name*

no time-range *name*

Syntax Description

name	Name of the time range. The name must be 64 characters or less.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Creating a time range does not restrict access to the device. The **time-range** command defines the time range only. After a time range is defined, you can attach it to traffic rules or an action.

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

The time range relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.

Examples

The following example creates a time range named “New_York_Minute” and enters time range configuration mode:

```
hostname(config)# time-range New_York_Minute
hostname(config-time-range)#
```

After you have created a time range and entered time-range configuration mode, you can define time range parameters with the **absolute** and **periodic** commands. To restore default settings for the **time-range** command **absolute** and **periodic** keywords, use the **default** command in time-range configuration mode.

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended** command to bind the time range to an ACL. The following example binds an ACL named "Sales" to a time range named "New_York_Minute":

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

See the **access-list extended** command for more information about ACLs.

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the security appliance.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.

timeout secure-phones

To configure the idle timeout after which the secure-phone entry is removed from the Phone Proxy database, use the **timeout secure-phones** command in phone-proxy configuration mode. To set the timeout value back to the default of 5 minutes, use the **no** form of this command.

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

Syntax Description

hh:mm:ss	Specifies the idle timeout after which the object is removed. The default is 5 minutes.

Defaults

The default value for secure phone timeout is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Since secure phones always request a CTL file upon bootup, the Phone Proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). The entry's timestamp is updated for each registration refresh the Phone Proxy receives for SIP phones and KeepAlives for SCCP phones.

The default value for the **timeout secure-phones** command is 5 minutes. Specify a value that is greater than the maximum timeout value for SCCP KeepAlives and SIP Register refresh. For example, if the SCCP Keepalives are configured for 1 minute intervals and the SIP Register Refresh is configured for 3 minutes, configure this timeout value greater than 3 minutes.

Examples

The following example shows the use of the **timeout secure-phones** command to configure the Phone Proxy to timeout entries in the secure phone database after 3 minutes:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
```

```
hostname(config-phone-proxy)# timeout secure-phones 00:03:00
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

timers lsa-group-pacing

To specify the interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

Syntax Description

seconds	The interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged. Valid values are from 10 to 1800 seconds.

Defaults

The default interval is 240 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To change the interval at which the OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** *seconds* command. To return to the default timer values, use the **no timers lsa-group-pacing** command.

Examples

The following example sets the group processing interval of LSAs to 500 seconds:

```
hostname(config-router)# timers lsa-group-pacing 500
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers spf	Specifies the shortest path first (SPF) calculation delay and hold time

timers spf

To specify the shortest path first (SPF) calculation delay and hold time, use the **timers spf** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

Syntax Description

delay	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds, from 1 to 65535.
holdtime	The hold time between two consecutive SPF calculations in seconds; valid values are from 1 to 65535.

Defaults

The defaults are as follows:

- *delay* is 5 seconds.
- *holdtime* is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To configure the delay time between when the OSPF protocol receives a topology change and when it starts a calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** command. To return to the default timer values, use the **no timers spf** command.

Examples

The following example sets the SPF calculation delay to 10 seconds and the SPF calculation hold time to 20 seconds:

```
hostname(config-router)# timers spf 10 20
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers lsa-group-pacing	Specifies the interval at which OSPF link-state advertisements (LSAs) are collected and refreshed, checksummed, or aged.

title

To customize the title of the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **title** command from webvpn customization mode:

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is “WebVPN Service”.

The default title style is:

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

To have no title, use the **title text** command without a *value* argument.

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the title is customized with the text "Cisco WebVPN Service":

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

tls-proxy

To configure a TLS proxy instance in TLS configuration mode or to set the maximum sessions, use the **tls-proxy** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

Syntax Description

max_sessions *max_sessions*	Specifies the maximum number of TLS proxy sessions to support on the platform.
noconfirm	Runs the **tls-proxy** command without requiring confirmation.
proxy_name	Specifies the name of the TLS proxy instance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **tls-proxy** command to enter TLS proxy configuration mode to create a TLS proxy instance, or to set the maximum sessions supported on the platform.

Examples

The following example shows how to create a TLS proxy instance:

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.

tos

To define a type of service byte in the IP header of an SLA operation request packet, use the **tos** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number	The service type value to be used in the IP header. Valid values are from 0 to 255.

Defaults

The default type of service value is 0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This field contains information such as delay, precedence, reliability, and so on. This is can be used by other routers on the network for policy routing and features such as Committed Access Rate.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes, the number of echo requests sent during an SLA operation to 5, and the type of service byte to 80.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# tos 80
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the request packet payload.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

traceroute

To determine the route packets will take to their destination, use the **traceroute** command.

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

Syntax Description

destination_ip	Specifies the destination IP address for the traceroute.
hostname	The hostname of the host to which the route has to be traced. If the hostname is specified, define it with the **name** command, or configure a DNS server to enable traceroute to resolve the hostname to an IP address. Supports DNS domain names such as www.example.com.
source	Specifies an IP address or interface is used as the source for the trace packets.
source_ip	Specifies the source IP address for the packet trace. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the security appliance.
source_interface	Specifies the source interface for the packet trace. When specified, the IP address of the source interface is used.
numeric	Specifies the output print only the IP addresses of the intermediate gateways. If this keyword is not specified the traceroute attempts to look up the hostnames of the gateways reached during the trace.
timeout	Specifies a timeout value is used
timeout_value	Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
probe *probe_num*	The number of probes to be sent at each TTL level. The default count is 3.
ttl	Keyword to specify the range of Time To Live values to use in the probes.
min_ttl	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
max-ttl	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
port *port_value*	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
use-icmp	Specifies the use of ICMP probe packets instead of UDP probe packets.

Defaults

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Priveleged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The traceroute command prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the **traceroute** command:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachablee.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Examples

The following example shows traceroute output that results when a destination IP address has been specified:

```
hostname# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.
packet-tracer	Enables packet tracing capabilities.

track rtr

To track the reachability of an SLA operation, use the **track rtr** command in global configuration mode. To remove the SLA tracking, use the **no** form of this command.

track *track-id* **rtr** *sla-id* **reachabilitity**

no track *track-id* **rtr** *sla-id* **reachabilitity**

Syntax Description

reachability	Specifies that the reachability of the object is being tracked.
sla-id	The ID of the SLA used by the tracking entry.
track-id	Creates a tracking entry object ID. Valid values are from 1 to 500.

Defaults

SLA tracking is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **track rtr** command creates a tracking entry object ID and specifies the SLA used by that tracking entry.

Every SLA operation maintains an operation return-code value, which is interpreted by the tracking process. The return code may be OK, Over Threshold, or several other return codes. Table 32-4 displays the reachability state of an object with respect to these return codes.

Table 32-4 SLA Tracking Return Codes

Tracking	Return Code	Track State
Reachability	OK or Over Threshold	Up
	Any other code	Down

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
hostname(config)# sla monitor 123
```

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
route	Configures a static route.
sla monitor	Defines an SLA monitoring operation.

traffic-non-sip

To allow non-SIP traffic using the well-known SIP signaling port, use the **traffic-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

traffic-non-sip

no traffic-non-sip

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to allow non-SIP traffic using the well-known SIP signaling port in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# traffic-non-sip
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

transfer-encoding

To restrict HTTP traffic by specifying a transfer encoding type, use the **transfer-encoding** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of this command.

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a connection using the specified transfer encoding type is detected.
allow	Allows the message.
chunked	Identifies the transfer encoding type in which the message body is transferred as a series of chunks.
compress	Identifies the transfer encoding type in which the message body is transferred using UNIX file compression.
default	Specifies the default action taken by the security appliance when the traffic contains a supported request method that is not on a configured list.
deflate	Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951).
drop	Closes the connection.
gzip	Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952).
identity	Identifies connections in which the message body is no transfer encoding is performed.
log	(Optional) Generates a syslog.
reset	Sends a TCP reset message to client and server.
type	Specifies the type of transfer encoding to be controlled through HTTP application inspection.

Defaults

This command is disabled by default. When the command is enabled and a supported transfer encoding type is not specified, the default action is to allow the connection without logging. To change the default action, use the **default** keyword and specify a different default action.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you enable the **transfer-encoding** command, the security appliance applies the specified action to HTTP connections for each supported and configured transfer encoding type.

The security appliance applies the **default** action to all traffic that does *not* match the transfer encoding types on the configured list. The preconfigured **default** action is to **allow** connections without logging.

For example, given the preconfigured default action, if you specify one or more encoding types with the action of **drop** and **log**, the security appliance drops connections containing the configured encoding types, logs each connection, and allows all connections for the other supported encoding types.

If you want to configure a more restrictive policy, change the default action to **drop** (or **reset**) and **log** (if you want to log the event). Then configure each permitted encoding type with the **allow** action.

Enter the **transfer-encoding** command once for each setting you wish to apply. You use one instance of the **transfer-encoding** command to change the default action and one instance to add each encoding type to the list of configured transfer encoding types.

When you use the **no** form of this command to remove an application category from the list of configured application types, any characters in the command line after the application category keyword are ignored.

Examples

The following example provides a permissive policy, using the preconfigured default, which allows all supported application types that are not specifically prohibited.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# transfer-encoding gzip drop log
hostname(config-http-map)#
```

In this case, only connections using GNU zip are dropped and the event is logged.

The following example provides a restrictive policy, with the default action changed to reset the connection and to log the event for any encoding type that is not specifically allowed.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse identity allow
hostname(config-http-map)#
```

In this case, only connections using no transfer encoding are allowed. When HTTP traffic for the other supported encoding types is received, the security appliance resets the connection and creates a syslog entry.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

trust-point

To specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer, use the **trust-point** command in tunnel-group ipsec-attributes mode. To eliminate a trustpoint specification, use the **no** form of this command.

trust-point *trust-point-name*

no trust-point *trust-point-name*

Syntax Description

trust-point-name	Specifies the name of the trustpoint to use.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group ipsec attributes	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all IPSec tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, configures a trustpoint for identifying the certificate to be sent to the IKE peer for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

trustpoint (SSO Server)

To specify the name of a trustpoint that identifies the certificate to be sent to the SAML POST-type SSO server, use the **trustpoint** command in config-webvpn-sso-saml mode. To eliminate a trustpoint specification, use the **no** form of this command.

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the name of the trustpoint to use.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Config webvpn sso saml	•	—	•	—	—

Command History

Release	Modification
7.3	This command is introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

Examples

The following example enters config-webvpn-sso-saml mode and names a trustpoint for identifying the certificate to be sent to the SAML POST type SSO Server:

```
hostname(config-webvpn)# sso server
hostname(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

Related Commands

Command	Description
crypto ca trustpoint	Manages trustpoint information.
show webvpn sso server	Displays the operating statistics for all SSO servers configured on the security device.
sso server	Creates, names, and specifies type for an SSO server.

tsig enforced

To require a TSIG resource record to be present, use the **tsig enforced** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

Syntax Description

drop	Drops the packet if TSIG is not present.
log	Generates a system message log.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command enables monitoring and enforcement of TSIG presence in DNS transactions.

Examples

The following example shows how to enable TSIG enforcement in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tsig enforced action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

ttl-evasion-protection

To disable the Time-To-Live evasion protection, use the **ttl-evasion-protection** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

ttl-evasion-protection

no ttl-evasion-protection

Syntax Description

This command has no arguments or keywords.

Defaults

TTL evasion protection offered by the security appliance is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **ttl-evasion-protection** command in tcp-map configuration mode to prevent attacks that attempt to evade security policy.

For instance, an attacker can send a packet that passes policy with a very short TTL. When the TTL goes to zero, a router between the security appliance and the endpoint drops the packet. It is at this point that the attacker can send a malicious packet with a long TTL that appears to the security appliance to be a retransmission and is passed. To the endpoint host, however, it is the first packet that has been received by the attacker. In this case, an attacker is able to succeed without security preventing the attack. Enabling this feature prevents such attacks.

Examples

The following example shows how to disable TTL evasion protection on flows from network 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# ttl-evasion-protection disable
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

tunnel-group

To create and manage the database of connection-specific records for IPSec and WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

tunnel-group *name* **type** *type*

no tunnel-group *name*

Syntax Description

name	Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.
type	Specifies the type of tunnel group: • remote-access—Allows a user to connect using either IPSec remote access or WebVPN (portal or tunnel client). • ipsec-l2l—Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet. **Note** The following tunnel-group types are deprecated in Release 8.0(2): ipsec-ra—IPSec remote access webvpn—WebVPN The security appliance converts these to the remote-access type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	See Note.	•	—	—

Note The tunnel-group command is available in transparent firewall mode to allow configuration of a LAN-to-LAN tunnel group, but not a remote-access group or a WebVPN group. All the tunnel-group commands that are available for LAN-to-LAN are also available in transparent firewall mode.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added webvpn type.
8.0(2)	Added remote-access type and deprecated ipsec-ra and webvpn types.

Usage Guidelines

The security appliance has the following default tunnel groups:

- DefaultRAGroup, the default IPSec remote-access tunnel group
- DefaultL2LGroup, the default IPSec LAN-to-LAN tunnel group
- DefaultWEBVPNGroup, the default WebVPN tunnel group.

You can change these groups, but not delete them. The security appliance uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

After entering the **tunnel-group** command, you enter the appropriate following commands to configure specific attributes for a particular tunnel group. Each of these commands enters a configuration mode for configuring tunnel-group attributes.

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

Examples

The following examples are entered in global configuration mode. The first configures a remote access tunnel group. The group name is group1.

```
hostname(config)# tunnel-group group1 type remote-access
hostname(config)#
```

The following example shows the tunnel-group command configuring the webvpn tunnel group named “group1”. You enter this command in global configuration mode:

```
hostname(config)# tunnel-group group1 type webvpn
hostname(config)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Enters the config-general mode for configuring general tunnel-group attributes
tunnel-group ipsec-attributes	Enters the config-ipsec mode for configuring IPSec tunnel-group attributes.
tunnel-group ppp-attributes	Enters the config-ppp mode for configuring PPP settings for L2TP connections.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

tunnel-group general-attributes

To enter the general-attribute configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

Syntax Description

general-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Various attributes from other tunnel-group types migrated to the general tunnel-group attributes list, and the prompt for tunnel-group general-attributes mode changed.

Examples

The following example entered in global configuration mode, creates a remote-access tunnel group for a remote-access connection using the IP address of the LAN-to-LAN peer, then enters general-attributes configuration mode for configuring tunnel-group general attributes. The name of the tunnel group is 209.165.200.225.

```
hostname(config)# tunnel-group 209.165.200.225 type remote-access
hostname(config)# tunnel-group 209.165.200.225 general-attributes
hostname(config-tunnel-general)#
```

The following example entered in global configuration mode, creates a tunnel group named” remotegrp” for an IPSec remote access connection, and then enters general configuration mode for configuring general attributes for the tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
```

```
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group ipsec-attributes

To enter the ipsec-attribute configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPSec tunneling protocol.

To remove all IPSec attributes, use the **no** form of this command.

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

Syntax Description

ipsec-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Various IPSec tunnel-group attributes migrated to the general tunnel-group attributes list, and the prompt for tunnel-group ipsec-attributes mode changed.

Examples

The following example entered in global configuration, creates a tunnel group for the IPSec remote-access tunnel group named remotegrp, and then specifies IPSec group attributes:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group ppp-attributes

To enter the ppp-attributes configuration mode and configure PPP settings that are used by L2TP over IPSec connections, use the **tunnel-group ppp-attributes** command in global configuration mode.

To remove all PPP attributes, use the **no** form of this command.

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

Syntax Description

name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

PPP settings are used by the Layer 2 Tunneling Protocol (L2TP), a VPN tunneling protocol which allows remote clients to use the dialup telephone service public IP network to securely communicate with private corporate network servers. L2TP is based on the client/server model and uses PPP over UDP (port 1701) to tunnel the data. All of the tunnel-group ppp commands are available for the PPPoE tunnel-group type.

Examples

The following example creates the tunnel group *telecommuters* and enters ppp-attributes configuration mode:

```
hostname(config)# tunnel-group telecommuters type pppoe
hostname(config)# tunnel-group telecommuters ppp-attributes
hostname(tunnel-group-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group webvpn-attributes

To enter the webvpn-attribute configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

Syntax Description

webvpn-attributes	Specifies WebVPN attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, creates a tunnel group for a WebVPN connection using the IP address of the LAN-to-LAN peer, then enters webvpn-configuration mode for configuring WebVPN attributes. The name of the tunnel group is 209.165.200.225.

```
hostname(config)# tunnel-group 209.165.200.225 type webvpn
hostname(config)# tunnel-group 209.165.200.225 webvpn-attributes
hostname(config-tunnel-webvpn)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for a WebVPN connection, and then enters webvpn configuration mode for configuring WebVPN attributes for the tunnel group named "remotegrp":

```
hostname(config)# tunnel-group remotegrp type webvpn
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group-map default-group

The **tunnel-group-map default-group** command specifies the default tunnel-group to use if the name could not be determined using other configured methods.

Use the **no** form of this command to eliminate a tunnel-group-map.

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

Syntax Description

default-group *tunnel-group-name*	Specifies a default tunnel group to use when the name cannot be derived by other configured methods. The *tunnel-group name* must already exist.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Defaults

The default value for the **tunnel-group-map default-group** is DefaultRAGroup.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The tunnel-group-map commands configure the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. To associate the certificate map entries, created using the **crypto ca certificate map** command, with tunnel groups, use the **tunnel-group-map** command in global configuration mode. You can invoke this command multiple times as long as each invocation is unique and you do not reference a map index more than once.

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

The processing that derives the tunnel-group name from the certificate ignores entries in the certificate map that are not associated with a tunnel group (any map rule not identified by this command).

Examples

The following example entered in global configuration mode, specifies a default tunnel group to use when the name cannot be derived by other configured methods. The name of the tunnel group to use is group1:

```
hostname(config)# tunnel-group-map default-group group1
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters crypto ca certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map enable	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups

tunnel-group-map enable

The **tunnel-group-map enable** command configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. Use the **no** form of this command to restore the default values.

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

Syntax Description

policy	Specifies the policy for deriving the tunnel group name from the certificate. *Policy* can be one of the following: **ike-id**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou, then the certificate-based IKE sessions are mapped to a tunnel group based on the content of the phase1 IKE ID. **ou**—Indicates that if a tunnel-group is not determined based on a rule lookup, then use the value of the organizational unit (OU) in the subject distinguished name (DN). **peer-ip**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou or ike-id methods, then use the established peer IP address. **rules**—Indicates that the certificate-based IKE sessions are mapped to a tunnel group based on the certificate map associations configured by this command.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Defaults

The default values for the **tunnel-group-map** command are **enable ou** and **default-group** set to DefaultRAGroup.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

Examples

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the content of the phase1 IKE ID:

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the established IP address of the peer:

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions based on the organizational unit (OU) in the subject distinguished name (DN):

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions based on established rules:

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-limit

To specify the maximum number of GTP tunnels allowed to be active on the security appliance, use the **tunnel limit** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** to set the tunnel limit back to its default.

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

Syntax Description

max_tunnels	This is the maximum number of tunnels allowed. The ranges is from 1 to 4294967295 for the global overall tunnel limit.

Defaults

The default for the tunnel limit is 500.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

New requests will be dropped once the number of tunnels specified by this command is reached.

Examples

The following example specifies a maximum of 10,000 tunnels for GTP traffic:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.

Commands	Description
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

tx-ring-limit

To specify the depth of the priority queues, use the **tx-ring-limit** command in priority-queue mode. To remove this specification, use the **no** form of this command.

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears. The range of **tx-ring-limit** values is 3 through 128 packets on the PIX platform and 3 through 256 packets on the ASA platform.

Defaults

The default **tx-ring-limit** is 128 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Priority-queue	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The security appliance recognizes priority traffic and enforces appropriate Quality of Service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.

You must use the **priority-queue** command to create the priority queue for an interface before priority queuing takes effect. You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue mode, as shown by the prompt. In priority-queue mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best -effort) allowed to be buffered before dropping packets (**queue-limit** command).

Note You *must* configure the **priority-queue** command in order to enable priority queueing for the interface.

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop*. To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Note The upper limit of the range of values for the **queue-limit** and **tx-ring-limit** commands is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device. The range of **queue-limit** values is 0 through 2048 packets. The range of **tx-ring-limit** values is 3 through 128 packets on the PIX platform and 3 through 256 packets on the ASA platform.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue-limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 2048 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 2048
hostname(priority-queue)# tx-ring-limit 256
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current **priority-queue**, **queue-limit**, and **tx-ring-limit** command configuration values.

type echo

To configure the SLA operation as an echo response time probe operation, use the **type echo** command in SLA monitor configuration mode. To remove the type from teh SLA configuration, use the **no** form of this command.

type echo protocol ipIcmpEcho *target* interface *if-name*

no type echoprotocol ipIcmpEcho *target* interface *if-name*

Syntax Description

interface *if-name*	Specifies the interface name, as specified by the **nameif** command, of the interface used to send the echo request packets. The interface source address is used as the source address in the echo request packets.
protocol	The protocol keyword. The only value supported is **ipIcmpEcho**, which specifies using an IP/ICMP echo request for the echo operation.
target	The IP address or host name of the object being monitored.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
SLA monitor configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The default size of the payload of the ICMP packets is 28 bytes, creating a total ICMP packet size of 64 bytes. The payload size can be changed using the **request-data-size** command.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the payload for the SLA operation request packet.
sla monitor	Defines an SLA monitoring operation.

CHAPTER 33

undebug through zonelabs integrity ssl-client-authentication Commands

undebug

To disable the display of debug information in the current session, use the **undebug** command in privileged EXEC mode.

undebug {*command* | **all**}

Syntax Description

command	Disables debug for the specified command. See the Usage Guidelines for information about the supported commands.
all	Disables all debug output.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified. It includes additional debug keywords.

Usage Guidelines

The following commands can be used with the undebug command. For more information about debugging a specific command, or for the associated arguments and keywords for a specific **debug** command, see the entry for **debug** *command*.

- aaa—AAA information
- acl—ACL information
- all—All debugging
- appfw—Application firewall information
- arp—ARP including NP operations
- asdm—ASDM information
- auto-update—Auto-update information
- boot-mem—Boot memory calculation and set
- cifs—CIFS information
- cmgr—CMGR information
- context—Context information
- cplane—CP information

- crypto—Crypto information
- ctiqbe—CTIQBE information
- ctl-provider—CTL provider debugging information
- dap—DAP information
- dcerpc—DCERPC information
- ddns—Dynamic DNS information
- dhcpc—DHCP client information
- dhcpd—DHCP server information
- dhcprelay—DHCP Relay information
- disk—Disk information
- dns—DNS information
- eap—EAP information
- eigrp—EIGRP protocol information
- email—Email information
- entity—Entity MIB information
- eou—EAPoUDP information
- esmtp—ESMTP information
- fips—FIPS 140-2 information
- fixup—Fixup information
- fover—Failover information
- fsm—FSM information
- ftp—FTP information
- generic—Miscellaneous information
- gtp—GTP information
- h323—H323 information
- http—HTTP information
- icmp—ICMP information
- igmp—Internet Group Management Protocol
- ils—LDAP information
- im—IM inspection information
- imagemgr—Image Manager information
- inspect—inspect debugging information
- integrityfw—Integrity Firewall information
- ip—IP information
- ipsec-over-tcp—IPSec over TCP information
- ipsec-pass-thru—Inspect ipsec-pass-thru information
- ipv6—IPv6 information
- iua-proxy—IUA proxy information

- kerberos—KERBEROS information
- l2tp—L2TP information
- ldap—LDAP information
- mfib—Multicast forwarding information base
- mgcp—MGCP information
- module-boot—Service module boot information
- mrib—Multicast routing information base
- nac-framework—NAC-FRAMEWORK information
- netbios-inspect—NETBIOS inspect information
- npshim—NPSHIM information
- ntdomain—NT domain information
- ntp—NTP information
- ospf—OSPF information
- p2p—P2P inspection information
- parser—Parser information
- pim—Protocol Independent Multicast
- pix—PIX information
- ppp—PPP information
- pppoe—PPPoE information
- pptp—PPTP information
- radius—RADIUS information
- redundant-interface—redundant interface information
- rip—RIP information
- rtp—RTP information
- rtsp—RTSP information
- sdi—SDI information
- sequence—Add sequence number
- session-command—Session command information
- sip—SIP information
- skinny—Skinny information
- sla—IP SLA Monitor Debug
- smtp-client—Email system log messsages
- splitdns—Split DNS information
- sqlnet—SQLNET information
- ssh—SSH information
- sunrpc—SUNRPC information
- tacacs—TACACS information
- tcp—TCP for WebVPN

- tcp-map—TCP map information
- timestamps—Add timestamp
- track—static route tracking
- vlan-mapping—VLAN mapping information
- vpn-sessiondb—VPN session database information
- vpnlb—VPN load balancing information
- wccp—WCCP information
- webvpn—WebVPN information
- xdmcp—XDMCP information
- xml—XML parser information

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The example disabled all debug output:

```
hostname(config)# undebug all
```

Related Commands

Command	Description
debug	Displays debug information for the selected command.

unix-auth-gid

To set the UNIX group ID, use the **unix-auth-gid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid <*identifier*>

no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Defaults

The default is 65534.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX group ID to 4567:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 4567
```

Related Commands

Command	Description
unix-auth-uid	Sets the UNIX user ID.

unix-auth-uid

To set the UNIX user ID, use the **unix-auth-uid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid <*identifier*>

no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Defaults

The default is 65534.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX user ID to 333:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# unix-auth-gid 333
```

Related Commands

Command	Description
unix-auth-gid	Sets the UNIX group ID.

upload-max-size

To specify the maximum size allowed for an object to upload, use the **upload-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

upload-max-size <*size*>

no upload-max-size

Syntax Description

size	Specifies the maximum size allowed for a uploaded object. The range is 0 through 2147483647.

Defaults

The default size is 2147483647.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn configuration mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Setting the size to 0 effectively disallows object uploading.

Examples

The following example sets the maximum size for a uploaded object to 1500 bytes:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# upload-max-size 1500
```

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
download-max-size	Specifies the maximum size of an object to download.

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

urgent-flag

To allow or clear the URG pointer through the TCP normalizer, use the **urgent-flag** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

Syntax Description

allow	Allows the URG pointer through the TCP normalizer.
clear	Clears the URG pointer through the TCP normalizer.

Defaults

The urgent flag and urgent offset are clear by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the newTCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **urgent-flag** command in tcp-map configuration mode to allow the urgent flag.

The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore, end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks. The default behavior is to clear the URG flag and offset.

Examples

The following example shows how to allow the urgent flag:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

uri-non-sip

To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, use the **uri-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

Syntax Description

mask	Masks the non-SIP URIs.
log	Specifies standalone or additional log in case of violation.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to identify the non-SIP URIs present in the Alert-Info and Call-Info header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

url

To maintain the list of static URLs for retrieving CRLs, use the **url** command in crl configure configuration mode. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. To delete an existing URL, use the **no** form of this command.

url *index url*

no url *index url*

Syntax Description

index	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The security appliance tries the URL at index 1 first.
url	Specifies the URL from which to retrieve the CRL.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CRL configure configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

Examples

The following example enters ca-crl configuration mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL https://foobin.com from which to retrieve CRLs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
policy	Specifies the source for retrieving CRLs.

url-block

To manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server, use the **url-block** command. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

Syntax Description

block *block_buffer*	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks.
mempool-size *memory_pool_size*	Configures the maximum size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
url-size *long_url_size*	Configures the maximum allowed URL size in KB for each long URL being buffered. The permitted values, which specifies a maximum URL size,: for Websense are 2, 3, or 4, representing 2 KB, 3 KB, or 4KB; or for Secure Computing, 2 or 3, representing 2 KB or 3 KB.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For Websense filtering servers, the **url-block url-size** command allows filtering of long URLs, up to 4 KB. For Secure Computing, the **url-block url-size** command allows filtering of long URLs, up to 3 KB. For both Websense and N2H2 filtering servers, the **url-block block** command causes the security appliance to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default security appliance behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the **url-block block** command and the filtering server permits the connection, the security appliance sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the security appliance sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the **url-block block** command to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block url-size** command with the **url-block mempool-size** command to specify the maximum length of a URL to be filtered and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense or Secure-Computing server. The **url-block url-size** command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense or Secure-Computing server (through a TCP packet stream) so that the Websense or Secure-Computing server can grant or deny access to that URL.

Examples

The following example assigns 56 1550-byte blocks for buffering responses from the URL filtering server:

```
hostname#(config)# url-block block 56
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

url-cache

To enable URL caching for URL responses received from a Websense server and to set the size of the cache, use the **url-cache** command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

no url-cache { **dst** | **src_dst** } *kbytes* [**kb**]

Syntax Description

dst	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the Websense server.
size *kbytes*	Specifies a value for the cache size within the range 1 to 128 KB.
src_dst	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the Websense server.
statistics	Use the **statistics** option to display additional URL cache statistics, including the number of cache lookups and hit rate.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Note The N2H2 server application does not support this command for url filtering.

The **url-cache** command provides a configuration option to cache responses from the URL server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Caching stores URL access privileges in memory on the security appliance. When a host requests a connection, the security appliance first looks in the URL cache for matching access privileges instead of forwarding the request to the Websense server. Disable caching with the **no url-cache** command.

Note If you change settings on the Websense server, disable the cache with the **no url-cache** command and then re-enable the cache with the **url-cache** command.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 URL filtering while using the **url-cache** command.

Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
hostname(config)# url-cache src_dst 128
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for URL responses received from a Websense filtering server.
url-server	Identifies a Websense server for use with the **filter** command.

url-entry

To enable or disable the ability to enter any HTTP/HTTPS URL on the portal page, use the **url-entry** command in dap webvpn configuration mode.

url-entry enable | disable

enable | disable	Enables or disables the ability to browse for file servers or shares..

Defaults

No default value or behaviors.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable URL entryfor the DAP record called Finance:

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dynamic-access-policy-record)# url-entry enable
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

url-length-limit

To configure the maximum length of the URL allowed in the RTSP message, use the **url-length-limit** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

url-length-limit *length*

no url-length-limit *length*

Syntax Description

length	The URL length limit in bytes. Range is 0 to 6000.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following example shows how to configure the URL length limit in an RTSP inspection policy map:

```
hostname(config)# policy-map type inspect rtsp rtsp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# url-length-limit 50
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

url-list (removed)

You can no longer use this command to define URl lists for access over SSL VPN connections. Now use the **import** command to import the XML object that defines a URL list. See the **import-** and **export-url-list** commands for more information.

Defaults

There is no default URL list.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration mode	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	This command was deprecated. It remains in the software for this release only to provide backward compatibility for pre-existing URL lists, so that the security appliance can convert such lists to XML files. Be aware that you cannot use the command to create a new URL list.

Usage Guidelines

You use the url-list command in global configuration mode to create one or more lists of URLs. To allow access to the URLs in a list for a specific group policy or user, use the *listname* you create here with the **url-list** command in webvpn mode.

Examples

The following example shows how to create a URL list called *Marketing URLs* that provides access to www.cisco.com, www.example.com, and www.example.org. The following table provides values that the example uses for each application.

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

Related Commands

Command	Description
clear configuration url-list	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
show running-configuration url-list	Displays the current set of configured urls.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

url-list (group-policy webvpn)

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a url list, use the **url-list none** command. Using the command a second time overrides the previous setting.

url-list {**value** *name* | **none**} [*index*]

no url-list

Syntax Description

index	Indicates the display priority on the home page.
none	Sets a null value for url lists. Prevents inheriting a list from a default or specified group policy.
value *name*	Specifies the name of a previously configured list of urls. To configure such a list, use the **url-list** command in global configuration mode.

Defaults

There is no default URL list.

Command Modes

The following table shows the modes in which you enter the commands:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy webvpn mode	•	—	•	—	—
Username mode	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list via an XML object. Use the **import** command in global configuration mode to download a URL list to the security appliance. Then use the url-list command to apply a list to a particular group policy or user.

Examples

The following example applies a URL list called FirstGroupURLs for the group policy named FirstGroup and assigns it first place among the URL lists:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

Related Commands

Command	Description
clear configure url-list [*listname*]	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
show running-configuration url-list	Displays the current set of configured **url-list** commands.
webvpn	Lets you enter webvpn mode. This can be webvpn configuration mode, group-policy webvpn configuration mode (to configure webvpn settings for a specific group policy), or username webvpn configuration mode (to configure webvpn settings for a specific user).

url-server

To identify an N2H2 or Websense server for use with the **filter** command, use the **url-server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

N2H2

url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

no url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

Syntax Description

N2H2

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	(Optional) The network interface where the authentication server resides. If not specified, the default is inside.
port *number*	The N2H2 server port. The security appliance also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP.
timeout *seconds*	The maximum idle time permitted before the security appliance switches to the next server you specified. The default is 30 seconds.
vendor	Indicates URL filtering service, using either ‘smartfilter’ or ‘n2h2’ (for backward compatibility); however, ‘smartfilter’ is saved as the vendor string.

Websense

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	The network interface where the authentication server resides. If not specified, the default is inside.

timeout *seconds*	The maximum idle time permitted before the security appliance switches to the next server you specified. The default is 30 seconds.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP protocol, Version 1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol Version **1** or **4**. The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•		•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **url-server** command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers in single context mode and 4 URL servers in multi mode; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the security appliance does not update the configuration on the application server; this must be done separately, according to the vendor instructions.

The **url-server** command must be configured before issuing the **filter** command for HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

Once you designate the server, enable the URL filtering service with the **filter url** command.

Use the **show url-server statistics** command to view server statistic information including unreachable servers.

Follow these steps to filter URLs:

Step 1 Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.

Step 2 Enable URL filtering with the **filter** command.

Step 3 (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.

Step 4 (Optional) Enable long URL and HTTP buffering support using the **url-block** command.

Step 5 Use the **show url-block block statistics**, **show url-cache statistics**, or the **show url-server statistics** commands to view run information.

For more information about Filtering by N2H2, visit N2H2's website at:

http://www.n2h2.com

For more information on Websense filtering services, visit the following website:

http://www.websense.com/

Examples

Using N2H2, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for URL responses received from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

user-authentication {**enable | disable**}

no user-authentication

Syntax Description

disable	Disables user authentication.
enable	Enables user authentication.

Defaults

User authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Individual users authenticate according to the order of authentication servers that you configure.

If you require user authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable user authentication for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
secure-unit-authentication	Provides additional security by requiring the VPN client to authenticate with a username and password each time the client initiates a tunnel.
user-authentication-idle-timeout	Sets an idle timeout for individual users. If there is no communication activity on a user connection in the idle timeout period, the security appliance terminates the connection.

user-authentication-idle-timeout

To set an idle timeout for individual users behind hardware clients, use the **user-authentication-idle-timeout** command in group-policy configuration mode. To delete the idle timeout value, use the **no** form of this command. This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, use the **user-authentication-idle-timeout none** command.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the security appliance terminates the connection.

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the idle timeout period. The range is from 1 through 35791394 minutes
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting an user authentication idle timeout value from a default or specified group policy.

Defaults

30 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

This timer terminates only the client's access through the VPN tunnel, not the VPN tunnel itself.

The idle timeout indicated in response to the **show uauth** command is always the idle timeout value of the user who authenticated the tunnel on the Cisco Easy VPN remote device.

Examples

The following example shows how to set an idle timeout value of 45 minutes for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

Related Commands

Command	Description
user-authentication	Requires users behind hardware clients to identify themselves to the security appliance before connecting.

user-storage

To store personalized user information between clientless SSL VPN sessions, use the **user storage** command in group-policy webvpn mode. To disable user storage, use the **no** versionof the command.

user-storage *NETFS-location*

no user-storage]

Syntax Description

NETFS-location	Specifies a file system desination in the form proto://user:password@host:port/path

Defaults

User storage is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Although the username, password, and preshared key are shown in the configuration, this poses no security risk because the security appliance stores this information in encrypted form, using an internal algorithm.

Examples

The following example shows how to set user storage for a user called newuser with a password of 12345678 at a file share called anyshare, and a path of anyfiler02a/new_share:

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

Related Commands

Command	Description
storage-key	
storage-objects	

username

To add a user to the security appliance database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **no** version of this command without appending a username.

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

no username *name*

Syntax Description

encrypted	Indicates that the password is encrypted (if you did not specify **mschap**). When you define a password in the **username** command, the security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** display would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s encrypted` The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another security appliance and you are using the same password.
mschap	Specifies that the password will be converted to unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using MSCHAPv1 or MSCHAPv2.
name	Specifies the name of the user as a string from 4 to 15 characters in length.
nopassword	Indicates that this user needs no password.
nt-encrypted	Indicates that the password is encrypted for use with MSCHAPv1 or MSCHAPv2. If you specified the **mschap** keyword when you added the user, then this keyword is displayed instead of the **encrypted** keyword when you view the configuration using the **show running-config** command. When you define a password in the **username** command, the security appliance encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **nt-encrypted** keword. For example, if you enter the password "test," the **show running-config** display would appear to be something like the following: `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` The only time you would actually enter the **nt-encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another security appliance and you are using the same password.
password *password*	Sets the password as a string from 3 to 16 characters in length.
privilege *priv_level*	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

Defaults

The default privilege level is 2.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0.1	This command was introduced.
7.2(1)	The **mschap** and **nt-encrypted** keywords were added.

Usage Guidelines

The **login** command uses this database for authentication.

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. (See the **aaa authorization command** command.) Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use AAA authentication so the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the **enable** password to access privileged EXEC mode.

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the **username attributes** command.

Examples

The following example shows how to configure a user named “anyuser” with a password of 12345678 and a privilege level of 12:

```
hostname(config)# username anyuser password 12345678 privilege 12
```

Related Commands

Command	Description
aaa authorization command	Configues command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username-from-certificate

To specify the field in a certificate to use as the username for authorization, use the **username-from-certificate** command in tunnel-group general-attributes mode. The DN of the peer certificate used as username for authorization

To remove the attribute from the configuration and restore default values, use the **no** form of this command.

username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no username-from-certificate

Syntax Description

primary-attr	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enable, the derived name can also be used in an authentication query.
use-entire-name	Specifies that the security appliance must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.

Defaults

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

This command selects the field in the certificate to use as the username. It replaces the deprecated **authorization-dn-attributes** command in Release 8.0.4 and following. The **username-from-certificate** command forces the security appliance to use the specified certificate field as the username for username/password authorization.

To use this derived username in the pre-fill username from certificate feature for username/passwordauthentication or authorization, you must also configure the **pre-fill-username** command in tunnel-group webvpn-attributes mode. That is, to use the pre-fill username feature, you must configure both commands.

Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.
use-entire-name	Use entire DN name. Not available a s a secondary attribute.

Examples

The following example, entered in global configuration mode, creates an IPSec remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute and OU as the secondary attribute to use to derive a name for an authorization query from a digital certificate:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN OU
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure Attribute-Value Pairs for a specified user.

username {*name*} **attributes**

no username [*name*] **attributes**

Syntax Description

name	Provides the name of the user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The internal user authentication database consists of the users entered with the username command. The login command uses this database for authentication. You can configure the username attributes using either the **username** command or the **username attributes** command.

The syntax of the commands in config-username mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration.
- The **none** keyword also removes the attribute from the running configuration. But it does so by setting the attribute to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

The **username attributes** command enters config-username mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Name an existing tunnel-group with which the user is required to connect.
password-storage	Enables/disables storage of the login password on the client system.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL
vpn-framed-ip-address	Specifies the IP address and the net mask to be assigned to the client.
vpn-group-policy	Specifies the name of a group-policy from which to inherit attributes.
vpn-idle-timeout	Specifies the idle timeout period in minutes, or **none** to disable.
vpn-session-timeout	Specifies the maximum user connection time in minutes, or **none** for unlimited time.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters webvpn mode, in which you configure webvpn attributes.

You configure webvpn-mode attributes for the username by entering the **username attributes** command and then entering the **webvpn** command in username webvpn configuration mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter username attributes configuration mode for a user named "anyuser":

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

Related Commands

Command	Description
clear config username	Clears the username database.
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the security appliance database.
webvpn	Enters username webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

username-prompt

To customize the username prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **username-prompt** command from webvpn customization mode:

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default is text of the username prompt is “USERNAME:”.

The default style of the username prompt is color:black;font-weight:bold;text-align:right.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Username:", and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page.
password-prompt	Customizes the password prompt of the WebVPN page.

user-alert

To enable broadcse an urgent message to all clientless SSL VPN users with currently active session, use the **user-alert** command in privileged EXEC mode. To disable the message, use the **no** form of this command.

user-alert *string*

no user-alert

Syntax Description

string	An alpha-numeric

Defaults

No message.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

When you issue this command, end users see a pop-up browser window with the configured message. This command causes no change in the security appliance configuration file.

Examples

The following example shows how to enable DAP trace debugging:

```
hostname # We will reboot the security appliance at 11:00 p.m. EST time. We apologize for
any inconvenience.
hostname #
```

user-message

To specify a text message to display when a DAP record is selected, use the user-message command in dynamic-access-policy-record mode. To remove this message, use the **no** version of the command. If you use the command more than once for the same DAP record, the newer message replaces the previous message.

user-message *message*

no user-message

Syntax Description

message	The message for users assigned to this DAP record. Maximum 128 characters. If the message contains spaces, enclose it in double quotation marks.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Dynamic-access-policy- record	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

For a successful SSL VPN connection, the portal page displays a flashing, clickable icon that lets the user see the message(s) associated with the connection. If the connection is terminated from a DAP policy (action = terminate), and if there is a user message configured in that DAP record, then that message displays on the login screen.

If more than one DAP record applies to a connection, the security appliance combines the applicable user messages and displays them as a single string.

Examples

The following example shows how to set a user message of “Hello Money Managers” for the DAP record called Finance.

```
hostname (config) config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# user-message “Hello Money Managers”
hostname(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

user-parameter

To specify the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication, use the **user-parameter** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

user-parameter *name*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The name of the username parameter included in the HTTP POST request. The maximum name size is 128 characters.

Defaults

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.

Note At login, the user enters the actual name value which is entered into the HTTP POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies that the username parameter userid be included in the HTTP POST request used for SSO authentication:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
start-url	Specifies the URL at which to retrieve a pre-login cookie.

user-storage

To store personalized user information between clientless SSL VPN sessions, use the **user storage** command in group-policy webvpn mode. To disable user storage, use the **no** versionof the command.

user-storage *NETFS-location*

no user-storage]

Syntax Description

NETFS-location	Specifies a file system desination in the form proto://user:password@host:port/path

Defaults

User storage is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy webvpn mode	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Although the username, password, and preshared key are shown in the configuration, this poses no security risk because the security appliance stores this information in encrypted form, using an internal algorithm.

Examples

The following example shows how to set user storage for a user called newuser with a password of 12345678 at a file share called anyshare, and a path of anyfiler02a/new_share:

```
hostname(config)# wgroup-policy DFLTGrpPolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# user-storage cifs://newuser:12345678@anyfiler02a/new_share
hostname(config-group_webvpn)#
```

Related Commands

Command	Description
storage-key	
storage-objects	

validate-attribute

To validate RADIUS attributes when using RADIUS accounting, use the **validate attribute** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

Syntax Description

attribute_number	The RADIUS attribute to be validated with RADIUS accounting. Values range from 1-191. Vendor Specific Attributes are not supported.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

When this command is configured, the security appliance will also do a match on these attributes in addition to the Framed IP attribute. Multiple instances of this command are allowed.

You can find a list of RADIUS attribute types here:

http://www.iana.org/assignments/radius-types

Examples

The following example shows how to enable RADIUS accounting for the user name RADIUS attribute:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# validate attribute 1
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

validation-policy (crypto ca trustpoint)

To specify the conditions under which a trustpoint can be used to validate the certificates associated with an incoming user connection, use the **validation-policy command** in crypto ca trustpoint configuration mode. To specify that the trustpoint cannot be used for the named condition, use the **no** form of the command.

[no] validation-policy {ssl | ipsec} [no-chain] [subordinate-only]

Syntax Description

ipsec	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate IPSec connections.
no-chain	Disables the chaining of subordinate certificates that are not resident on the security device.
ssl	Specifies that the Certificate Authority (CA) certificate and policy associated with the trustpoint can be used to validate SSL connections.
subordinate-only	Disables validation of client certificates issued directly from the CA represented by this trustpoint.

Defaults

No default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command History

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Remote-access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPSec), or both, depending on deployment requirements, to permit access to virtually any network application or resource. The **validation-policy** command allows you to specify the protocol type permitted to access on-board CA certificates.

The **no-chain** option with this command prevents a security applicance from supporting subordinate CA certificates that are not configured as trustpoints on the security appliance.

The security appliance can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is disabled automatically if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint, central, and designates it an SSL trustpoint:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# validation-policy ssl
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for trustpoint, checkin1,and sets it to accept certificates that are subordinate to the specified trustpoint.

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# validation-policy subordinates-only
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

verify

To verify the checksum of a file, use the **verify** command in privileged EXEC mode.

verify *path*

verify /md5 *path* [*md5-value*]

Syntax Description

/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
md5-value	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system will calculate the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
path	• **disk0:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the internal Flash memory. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:**/[*path*/]*filename* This option is only available for the ASA 5500 series adaptive security appliance, and indicates the external Flash memory card. • **flash:**/[*path*/]*filename* This option indicates the internal Flash card. For the ASA 5500 series adaptive security appliance, **flash** is an alias for **disk0**. • **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*] The **type** can be one of the following keywords: – **ap**—ASCII passive mode – **an**—ASCII normal mode – **ip**—(Default) Binary passive mode – **in**—Binary normal mode • **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename* • **tftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;int=***interface_name*] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **verify** command.

Defaults

The current flash device is the default file system.

Note When you specify the **/md5** option, you can use a network file, such as ftp, http and tftp as the source. The **verify** command without the **/md5** option only lets you verify local images in Flash.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into Flash memory; it is not displayed when the image file is copied from one disk to another.

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into Flash memory or onto a server. A variety of image information is available on Cisco.com.

To display the contents of Flash memory, use the **show flash** command. The Flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into Flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the security appliance and saved in the file system without detection. If a corrupt image is transferred successfully to the security appliance, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of the security appliance software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all security appliance software images for comparison against local system image values.

To perform the MD5 integrity check, issue the **verify** command using the **/md5** keyword. For example, issuing the **verify /md5 flash:cdisk.bin** command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Examples

The following example shows the verify command used on an image file called cdisk.bin. Some of the text was removed for clarity:

```
hostname# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

version

To specify the version of RIP used globally by the security appliance, use the **version** command in router configuration mode. To restore the defaults, use the **no** form of this command.

version {**1** | **2**}

no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Defaults

The security appliance accepts Version 1 and Version 2 packets but sends only Version 1 packets.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip send version** and **rip receive version** commands on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the security appliance to send and receive RIP Version 2 packets on all interfaces:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.

virtual http

To configure a virtual HTTP server, use the **virtual http** command in global configuration mode. To disable the virtual server, use the **no** form of this command.

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

Syntax Description

ip_address	Sets the IP address for the virtual HTTP server on the security appliance. Make sure this address is an unused address that is routed to the security appliance.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the security appliance. This keyword applies only for text-based browsers, where the redirect cannot happen automatically.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was deprecated because the inline basic HTTP authentication method used in prior releases was replaced by the redirection method; this command was no longer needed.
7.2(2)	This command was revived because you can now choose between using basic HTTP authentication (the default) or using HTTP redirection using the **aaa authentication listener** command. The redirection method does not require an extra command for cascading HTTP authentications.

Usage Guidelines

When you use HTTP authentication on the security appliance (see the **aaa authentication match** or the **aaa authentication include** command), the security appliance uses basic HTTP authentication by default. You can change the authentication method so that the security appliance redirects HTTP connections to web pages generated by the security appliance itself using the **aaa authentication listener** command with the **redirect** keyword.

However, if you continue to use basic HTTP authentication, then you might need the **virtual http** command when you have cascading HTTP authentications.

If the destination HTTP server requires authentication in addition to the security appliance, then the **virtual http** command lets you authenticate separately with the security appliance (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

For inbound users (from lower security to higher security), you must also include the virtual HTTP address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual HTTP IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual HTTP address. A **static** statement is not required.

Note Do not set the **timeout uauth** command duration to 0 seconds when using the **virtual http** command, because this setting prevents HTTP connections to the real web server.

Examples

The following example shows how to enable virtual HTTP along with AAA authentication:

```
hostname(config)# virtual http 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list ACL-IN remark This is the HTTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list ACL-IN remark This is the virtual HTTP address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq http
hostname(config)# access-list AUTH remark This is the HTTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list AUTH remark This is the virtual HTTP address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
aaa authentication listener http	Sets the method by which the security appliance authentica
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the security appliance virtual server.

sysopt uauth allow-http-cache	When you enable the **virtual http** command, this command lets you use the username and password in the browser cache to reconnect to the virtual server.
virtual telnet	Provides a virtual Telnet server on the security appliance to let users authenticate with the security appliance before initiating other types of connections that require authentication.

virtual telnet

To configure a virtual Telnet server on the security appliance, use the **virtual telnet** command in global configuration mode. You might need to authenticate users with the virtual Telnet server if you require authentication for other types of traffic for which the security appliance does not supply an authentication prompt. To disable the server, use the **no** form of this command.

virtual telnet *ip_address*

no virtual telnet *ip_address*

Syntax Description

ip_address	Sets the IP address for the virtual Telnet server on the security appliance. Make sure this address is an unused address that is routed to the security appliance.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the security appliance, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

For inbound users (from lower security to higher security), you must also include the virtual Telnet address as a destination interface in the access list applied to the source interface. Moreover, you must add a **static** command for the virtual Telnet IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself).

For outbound users, there is an explicit permit for traffic, but if you apply an access list to an inside interface, be sure to allow access to the virtual Telnet address. A **static** statement is not required.

To logout from the security appliance, reconnect to the virtual Telnet IP address; you are prompted to log out.

Examples

This example shows how to enable virtual Telnet along with AAA authentication for other services:

```
hostname(config)# virtual telnet 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
hostname(config)# access-list ACL-IN remark This is the virtual Telnet address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
hostname(config)# access-list AUTH remark This is the virtual Telnet address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the security appliance virtual server.
virtual http	When you use HTTP authentication on the security appliance, and the HTTP server also requires authentication, this command allows you to authenticate separately with the security appliance and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

vlan

To assign a VLAN ID to a subinterface, use the **vlan** command in interface configuration mode. To remove a VLAN ID, use the **no** form of this command. Subinterfaces require a VLAN ID to pass traffic. VLAN subinterfaces let you configure multiple logical interfaces on a single physical interface. VLANs let you keep traffic separate on a given physical interface, for example, for multiple security contexts.

vlan *id*

no vlan

Syntax Description

id	Specifies an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the security appliance changes the old ID.

You need to enable the physical interface with the **no shutdown** command to let subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual.

The maximum number of subinterfaces varies depending on your platform. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for the maximum subinterfaces per platform.

Examples

The following example assigns VLAN 101 to a subinterface:

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example changes the VLAN to 102:

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the current configuration of the interface.

vlan (group-policy)

To assign a VLAN to a group policy, use the **vlan** command in group-policy configuration mode. To remove the VLAN from the configuration of the group policy and replace it with the VLAN setting of the default group policy, use the **no** form of this command.

[**no**] **vlan** {*vlan_id* |**none**}

Syntax Description

vlan_id	Number of the VLAN, in decimal format, to assign to remote access VPN sessions that use this group policy. The VLAN must be configured on this security appliance, using the **vlan** command in interface configuration mode.
none	Disables the assignment of a VLAN to the remote access VPN sessions that match this group policy. The group policy does not inherit the vlan value from the default group policy.

Defaults

The default value is none.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	This command was introduced.

Usage Guidelines

This command specifies the egress VLAN interface for sessions assigned to this group policy. The security appliance forwards all traffic on this group to that VLAN. You can assign a VLAN to each group policy to simplify access control. Use this command as an alternative to using ACLs to filter traffic on a session.

Examples

The following command assigns the VLAN 1 to the group policy:

```
hostname(config-group-policy)# vlan 1
hostname(config-group-policy)
```

The following command removes VLAN mapping from the group policy:

```
hostname(config-group-policy)# vlan none
hostname(config-group-policy)
```

Related commands

Command	Description
`show vlan`	Shows the VLANs configured on the security appliance.
`vlan` (interface configuration mode)	Assigns a VLAN ID to a subinterface.
`show vpn-session_summary.db`	Displays the number IPSec, Cisco AnyConnect, and NAC sessions, and the number of VLANs in use.
`show vpn-session.db`	Displays information about VPN sessions, including VLAN mapping and NAC results.

vpdn group

To create or edit a vpdn group and configure PPPoE client settings, use the **vpdn group** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

vpdn group *group_name* {**localname** *username* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** *name* | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

Note PPPoE is not supported when failover is configured on the security appliance, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

vpdn group *group_name*	Specifies a name for the vpdn group
localname *username*	Links the user name to the vpdn group for authentication, and must match the name configured with the **vpdn username** command.
request dialout pppoe	Specifies to allow dialout PPPoE requests.
**ppp authentication {chap | mschap | pap}}	Specifies the Point-to-Point Protocol (PPP) authentication protocol. The Windows client dial-up networking settings lets you specify what authentication protocol to use (PAP, CHAP, or MS-CHAP). Whatever you specify on the client must match the setting you use on the security appliance. Password Authentication Protocol (PAP) lets PPP peers authenticate each other. PAP passes the host name or username in clear text. Challenge Handshake Authentication Protocol (CHAP) lets PPP peers prevent unauthorized access through interaction with an access server. MS-CHAP is a Microsoft derivation of CHAP. PIX Firewall supports MS-CHAP Version 1 only (not Version 2.0). If an authentication protocol is not specified on the host, do not specify the **ppp authentication** option in your configuration.

Defaults

default behavior or values. See Usage Guidelines.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2.1	This command was introduced.

Usage Guidelines

Virtual Private Dial-up Networking (VPDN) is used to provide long distance, point-to-point connections between remote dial-in users and a private network. VDPN on the security appliance uses the Layer 2 tunnelling technology PPPoE to establish dial-up networking connections from the remote user to the private network across a public network.

PPPoE is the Point-to-Point Protocol (PPP) over Ethernet. PPP is designed to work with network layer protocols such as IP, IPX, and ARA. PPP also has CHAP and PAP as built-in security mechanisms.

The **show vpdn session pppoe** command displays session information for PPPOE connections. The **clear configure vpdn group** command removes all **vpdn group** commands from the configuration and stops all the active L2TP and PPPoE tunnels. The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Because PPPoE encapsulates PPP, PPPoE relies on PPP to perform authentication and ECP and CCP functions for client sessions operating within the VPN tunnel. Additionally, PPPoE is not supported in conjunction with DHCP because PPP assigns the IP address for PPPoE.

Note Unless the VPDN group for PPPoE is configured, PPPoE cannot establish a connection.

To define a VPDN group to be used for PPPoE, use the **vpdn group** *group_name* **request dialout pppoe** command. Then use the **pppoe client vpdn group** command from interface configuration mode to associate a VPDN group with a PPPoE client on a particular interface.

If your ISP requires authentication, use the **vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} command to select the authentication protocol used by your ISP.

Use the **vpdn group** *group_name* **localname** *username* command to associate the username assigned by your ISP with the VPDN group.

Use the **vpdn username** *username* password *password* command to create a username and password pair for the PPPoE connection. The username must be a username that is already associated with the VPDN group specified for PPPoE.

Note If your ISP is using CHAP or MS-CHAP, the username may be called the remote system name and the password may be called the CHAP secret.

The PPPoE client functionality is turned off by default, so after VPDN configuration, enable PPPoE with the **ip address** *if_name* **pppoe** [**setroute**] command. The **setroute** option causes a default route to be created if no default route exists.

As soon as PPPoE is configured, the security appliance attempts to find a PPPoE access concentrator with which to communicate. When a PPPoE connection is terminated, either normally or abnormally, the security appliance attempts to find a new access concentrator with which to communicate.

The following **ip address** commands should not be used after a PPPoE session is initiated because they will terminate the PPPoE session:

- **ip address outside pppoe**, because it attempts to initiate a new PPPoE session.
- **ip address outside dhcp**, because it disables the interface until the interface gets its DHCP configuration.
- **ip address outside** *address netmask*, because it brings up the interface as a normally initialized interface.

Examples

The following example creates a vdpn group *telecommuters* and configures the PPPoE client:

```
F1(config)# vpdn group telecommuters request dialout pppoe
F1(config)# vpdn group telecommuters localname user1
F1(config)# vpdn group telecommuters ppp authentication pap
F1(config)# vpdn username user1 password test1
F1(config)# interface GigabitEthernet 0/1
F1(config-subif)# ip address pppoe setroute
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configurations.
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show vpdn group *group_name*	Displays the vpdn group configuration.
vpdn username	Creates a username and password pair for the PPPoE connection.

vpdn username

To create a username and password pair for PPPoE connections, use the **vpdn username** command in global configuration mode.

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

Note PPPoE is not supported when failover is configured on the security appliance, or in multiple context or transparent mode. PPPoE is only supported in single, routed mode, without failover.

Syntax Description

username	Specifies the username.
password	Specifies the password.
store-local	Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

Defaults

No default behavior or values. See Usage Guidelines.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The vpdn username must be a username that is already associated with the VPDN group specified with the **vpdn group** *group_name* **localname** *username* command.

The **clear configure vpdn username** command removes all the **vpdn username** commands from the configuration.

Examples

The following example creates the vpdn username *bob_smith* with the password *telecommuter*9/8:

```
F1(config)# vpdn username bob_smith password telecommuter9/8
```

Related Commands

Command	Description
clear configure vpdn group	Removes all vpdn group commands from the configurations.
clear configure vpdn username	Removes all vpdn username commands from the configuration.
show vpdn group	Displays the vpdn group configuration.
vpdn group	Create a vpdn group and configures PPPoE client settings,

vpn-access-hours

To associate a group policy with a configured time-range policy, use the **vpn-access-hours** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, use the **vpn-access-hours none** command.

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

Syntax Description

none	Sets VPN access hours to a null value, thereby allowing no time-range policy. Prevents inheriting a value from a default or specified group policy.
time-range	Specifies the name of a configured time-range policy.

Defaults

Unrestricted.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

Related Commands

Command	Description
time-range	Sets days of the week and hours of the day for access to the network, including start and end dates.

vpn-addr-assign

To specify a method for assigning IP addresses to remote access clients, use the **vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all configured VPN address assignment methods from the security appliance, user the **no** version of this command. without arguments.

vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

no vpn-addr-assign {**aaa | dhcp | local** [**reuse-delay** *delay*]}

Syntax Description

aaa	Obtains IP addresses from an external AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from internal authentication server, and associates them with a tunnel group.
reuse-delay *delay*	The delay before a released IP address can be reused. The range is 0 to 480 minutes. The default is 0 (disabled).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0.3	The **reuse-delay** option was introduced.

Usage Guidelines

If you choose DHCP, you should also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use. You must use the **dhcp-server** command to indicate the IP addresses that the DHCP server uses.

If you choose local, you must also use the **ip-local-pool** command to define the range of IP addresses to use. You then use the **vpn-framed-ip-address** and **vpn-framed-netmask** commands to assign IP addresses and netmasks to individual users.

With the local pool, you can use the **reuse-delay** *delay* option to adjust the delay before a released IP address can be reused. Increasing the delay prevents problems firewalls may experience when an IP address is returned to the pool and reassigned quickly.

If you choose AAA, you obtain IP addresses from either a previously configured RADIUS server.

Examples

The following example shows how to configure DHCP as the address assignment method:

```
hostname(config)# vpn-addr-assign dhcp
```

Related Commands

Command	Description
dhcp-network-scope	Specifies the range of IP addresses the security appliance DHCP server should use to assign addresses to users of a group policy.
ip-local-pool	Creates a local IP address pool.
vpn-framed-ip-address	Specifies the IP address to assign to a particular user.
vpn-framed-ip-netmask	Specifies the netmask to assign to a particular user.

vpn-filter

To specify the name of the ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, including a null value created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those ACLs.

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

Syntax Description

none	Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *ACL name*	Provides the name of the previously configured access list.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The ACL defined in the **vpn-filter** command does not apply to clientless SSL VPN connections. It applies to IPsec and SSL VPN client sessions only.

Examples

The following example shows how to set a filter that invokes an access list named acl_vpn for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.

vpn-framed-ip-address

To specify the IP address to assign to a particular user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

Syntax Description

ip_address	Provides the IP address for this user.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

vpn-group-policy

To have a user inherit attributes from a configured group policy, use the **vpn-group-policy** command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

Syntax Description

group-policy name	Provides the name of the group policy.

Defaults

By default, VPN users have no group policy association.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can override the value of an attribute in a group policy for a particular user by configuring it in username mode, if that attribute is available in username mode.

Examples

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Adds a group policy to the security appliance database.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a group policy.

Command	Description
username	Adds a user to the security appliance database.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

vpn-idle-timeout

To configure a user timeout period use the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode. If there is no communication activity on the connection in this period, the security appliance terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

vpn-idle-timeout {*minutes* **| none}**

no vpn-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting a value from a default or specified group policy.

Defaults

30 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-session-timeout	Configures the maximum amount of time allowed for VPN connections. At the end of this period of time, the security appliance terminates the connection.

vpn load-balancing

To enter vpn load-balancing mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

vpn load-balancing

Note To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration mode	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(2)	Added support for ASA Model 5510 with a Plus license and models above 5520.

Usage Guidelines

A load-balancing cluster can include security appliance models 5510 (with a Plus license), or ASA 5520 and above. You can also include VPN 3000 Series Concentrators in the cluster. While mixed configurations are possible, administration is generally simpler if the cluster is homogeneous.

Use the **vpn load-balancing** command to enter vpn load-balancing mode. The following commands are available in vpn load-balancing mode:

- cluster encryption
- cluster ip address
- cluster key
- cluster port
- interface

- nat
- participate
- priority
- redirect-fqdn

See the individual command descriptions for detailed information.

Examples

The following is an example of the **vpn load-balancing** command; note the change in the prompt:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that specifies the public interface of the cluster as “test” and the private interface of the cluster as “foo”:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.

vpn-sessiondb logoff

To log off all or selected VPN sessions, use the **vpn-sessiondb logoff** command in global configuration mode.

vpn-sessiondb logoff {**remote | l2l | webvpn | email-proxy | protocol** *protocol-name* | **name** *username* **| ipaddress** *IPaddr* **| tunnel-group** *groupname* **| index** *indexnumber* | **all**}

Syntax Description

all	Logs off all VPN sessions.
email-proxy	Logs off all e-mail proxy sessions.
index *indexnumber*	Logs off a single session by index number. Specify the index number for the session.
ipaddress *IPaddr*	Logs off sessions for the IP address hat you specify.
l2l	Logs off all LAN-to-LAN sessions.
name *username*	Logs off sessions for the username that you specify.
protocol *protocol-name*	Logs off sessions for protocols that you specify. The protocols include: IKE — POP3S IMAP4S — SMTPS IPSec — userHTTPS IPSecLAN2LAN — vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	Logs off all remote-access sessions.
tunnel-group *groupname*	Logs off sessions for the tunnel group that you specify.
webvpn	Logs off all WebVPN sessions.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to log off all remote-access sessions:

```
hostname# vpn-sessiondb logoff remote
```

The next example shows how to log off all IPSec sessions:

hostname# **vpn-sessiondb logoff protocol IPSec**

vpn-sessiondb max-session-limit

To limit VPN sessions to a lower value than the security appliance allows, use the **vpn-sessiondb max-session-limit** command in global configuration mode. To remove the session limit, use the **no** version of this command. To overwrite the current setting, use the command again.

vpn-sessiondb max-session-limit {*session-limit*}

no **vpn-sessiondb max-session-limit**

Syntax Description

session-limit	Specifies the maximum number of VPN sessions permitted.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command applies to IPSec VPN sessions,.

Examples

The following example shows how to set a maximum VPN session limit of 450:

```
hostname# vpn-sessiondb max-session-limit 450
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-webvpn-session-limit	Sets a maximum number of WebVPN sessions.

vpn-sessiondb max-webvpn-session-limit

To limit SSL VPN sessions to a lower value than the security appliance allows, use the **vpn-sessiondb max-webvpn-session-limit** command in global configuration mode. To remove the session limit, use the **no** version of this command. To overwrite the current setting, use the command again.

vpn-sessiondb max-webvpn-session-limit {*session-limit*}

no vpn-sessiondb max-webvpn-session-limit

Syntax Description

session-limit	Specifies the maximum number of WebVPN sessions permitted.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

This command applies to SSL VPN sessions, including AnyConnect VPN Client, legacy SSL VPN Client (SVC), and clientless (formerly WebVPN) session.

Examples

The following example shows how to set a maximum session limit of 75:

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and SSL VPN sessions.
vpn-sessiondb max-vpn-session-limit	Sets a maximum number of VPN sessions.

vpn-session-timeout

To configure a maximum amount of time allowed for VPN connections, use the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode. At the end of this period of time, the security appliance terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-session-timeout none** command.

vpn-session-timeout {*minutes* **| none}**

no vpn-session-timeout

Syntax Description

minutes	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited session timeout period. Sets session timeout with a null value, thereby disallowing a session timeout. Prevents inheriting a value from a default or specified group policy.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-idle-timeout	Configures the user timeout period. If there is no communication activity on the connection in this period, the security appliance terminates the connection.

vpn-simultaneous-logins

To configure the number of simultaneous logins permitted for a user, use the **vpn-simultaneous-logins** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy. Enter 0 to disable login and prevent user access.

vpn-simultaneous-logins {*integer***}**

no vpn-simultaneous-logins

Syntax Description

integer	A number between 0 and 2147483647.

Defaults

The default is 3 simultaneous logins.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enter 0 to disable login and prevent user access.

Note While the maximum limit for the number of simultaneous logins is very large, allowing several simultaneous logins could compromise security and affect performance.

Stale AnyConnect, IPSec Client, or Clientless sessions (sessions that are terminated abnormally) might remain in the session database, even though a "new" session has been established with the same username.

If the value of vpn-simultaneous-logins is 1, and the same user logs in again after an abnormal termination, then the stale session is removed from the database and the new session is established. If, however, the existing session is still an active connection and the same user logs in again, perhaps from another PC, the first session is logged off and removed from the database, and the new session is established.

If the number of simultaneous logins is a value greater than 1, then, when you have reached that maximum number and try to log in again, the session with the longest idle time is logged off. If all current sessions have been idle an equally long time, then the oldest session is logged off. This action frees up a session and allows the new login.

Examples

The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

To configure a VPN tunnel type (IPSec, L2TP over IPSec, SVC, or WebVPN), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

no vpn-tunnel-protocol {**IPSec** | **l2tp-ipsec** | **svc** | **webvpn**}

Syntax Description

IPSec	Negotiates an IPSec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
l2tp-ipsec	Negotiates an IPSec tunnel for an L2TP connection.
svc	Negotiates an SSL VPN tunnel with an SSL VPN client.
webvpn	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

Defaults

The default is IPSec.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—
Username configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **l2tp-ipsec** keyword was added.
7.3(1)	The **svc** keyword was added.

Usage Guidelines

Use this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

Note To support fallback from IPSec to SSL, the **vpn-tunnel-protocol** command must have both the **svc** and **ipsec** arguments configured.

Examples

The following example shows how to configure WebVPN and IPSec tunneling modes for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

Related Commands

Command	Description
address pools	Specifies a list of address pools for allocating addresses to remote clients.
show running-config group-policy	Displays the configuration for all group-policies or for a specific group-policy.

vpnclient connect

To attempt to establish an Easy VPN Remote connection to the configured server or servers, use the **vpnclient connect** command in global configuration mode.

vpnclient connect

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Examples

The following example shows how to attempt to establish an Easy VPN Remote connection to a configured EasyVPN server:

```
hostname(config)# vpnclient connect
hostname(config)#
```

vpnclient disconnect

To disconnect Easy VPN Remote connection, use the **vpnclient disconnect** command in global configuration mode.

vpnclient disconnect

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Examples

The following example shows how to disconnect an Easy VPN Remote connection:

```
hostname(config)# vpnclient disconnect
hostname(config)#
```

vpnclient enable

To enable the Easy VPN Remote feature, use the **vpnclient enable** command in global configuration mode. To disable the Easy VPN Remote feature, use the **no** form of this command:

vpnclient enable

no vpnclient enable

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505.

If you enter the **vpnclient enable** command, the ASA 5505 functions as a Easy VPN hardware client (also called "Easy VPN Remote"). If you enter the **vpnclient enable** command, it functions as an Easy VPN server (also called a "headend"). It can function only as a client or a server.

Examples

The following example shows how to enable the Easy VPN Remote feature:

```
hostname(config)# vpnclient enable
hostname(config)#
```

The following example shows how to disable the Easy VPN Remote feature:

```
hostname(config)# no vpnclient enable
hostname(config)#
```

vpnclient ipsec-over-tcp

To configure the ASA 5505 running as an Easy VPN hardware client to use TCP-encapsulated IPSec, use the **vpnclient ipsec-over-tcp** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

Syntax Description

port	(Optional) Specifies the use of a particular port.
tcp_port	(Required if you specify the keyword **port**.) Specifies the TCP port number to be used for a TCP-encapsulated IPSec tunnel.

Defaults

The Easy VPN Remote connection uses port 10000 if the command does not specify a port number.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN hardware client (also called "Easy VPN Remote").

By default, the Easy VPN client and server encapsulate IPSec in User Datagram Protocol (UDP) packets. Some environments, such as those with certain firewall rules, or NAT and PAT devices, prohibit UDP. To use standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) in such environments, you must configure the client and the server to encapsulate IPSec within TCP packets to enable secure tunneling. If your environment allows UDP, however, configuring IPSec over TCP adds unnecessary overhead.

If you configure an ASA 5505 to use TCP-encapsulated IPSec, enter the following command to let it send large packets over the outside interface:

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

This command clears the Don't Fragment (DF) bit from the encapsulated header. A DF bit is a bit within the IP header that determines whether the packet can be fragmented. This command lets the Easy VPN hardware client send packets that are larger than the MTU size.

Examples

The following example shows how to configure the Easy VPN hardware client to use TCP-encapsulated IPSec, using the default port 10000, and to let it send large packets over the outside interface:

```
hostname(config)# vpnclient ipsec-over-tcp
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

The next example shows how to configure the Easy VPN hardware client to use TCP-encapsulated IPSec, using the port 10501, and to let it send large packets over the outside interface:

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

vpnclient mac-exempt

To exempt devices behind an Easy VPN Remote connection from individual user authentication requirements, use the **vpnclient mac-exempt** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

Syntax Description

mac_addr_1	MAC address, in dotted hexadecimal notation, specifying a manufacturer and serial number of a device for which to exempt individual user authentication. For more than one device, specify each MAC address, separating each with a space and the respective network mask. The first 6 characters of the MAC address identify the device manufacturer, and the last 6 characters are the serial number. The last 24 bits are the unit's serial number in hexadecimal format.
mac_mask_1	Network mask for the corresponding MAC address. Use a space to separate the network mask and any subsequent MAC address and network mask pairs.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Devices such as Cisco IP phones, wireless access points, and printers are incapable of performing authentication, and therefore do not authenticate when individual unit authentication is enabled. If individual user authentication is enabled, you can use this command to exempt such devices from authentication. The exemption of devices from individual user authentication is also called “device pass-through.”

The format for specifying the MAC address and mask in this command uses three hex digits, separated by periods; for example, the MAC mask ffff.ffff.ffff matches just the specified MAC address. A MAC mask of all zeroes matches no MAC address, and a MAC mask of ffff.ff00.0000 matches all devices made by the same manufacturer.

Examples

Cisco IP phones have the Manufacturer ID 00036b, so the following command exempts any Cisco IP phone, including Cisco IP phones, you might add in the future:

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

The next example provides greater security but less flexibility because it exempts one specific Cisco IP phone:

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

vpnclient management

To generate IPSec tunnels for management access to the Easy VPN hardware client, use the **vpnclient management** command in global configuration mode.

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management clear

To remove the attribute from the running configuration, use the **no** form of this command, which sets up IPSec tunnels exclusively for management in accordance with the **split-tunnel-policy** and **split-tunnel-network-list** commands.

no vpnclient management

Syntax Description

clear	Uses normal routing to provide management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client. This option does not create management tunnels. **Note** Use this option if a NAT device is operating between the client and the Internet.
ip_addr	IP address of the host or network for which to build a management tunnel from the Easy VPN hardware client. Use this argument with the **tunnel** keyword. Specify one or more IP addresses, separating each with a space and the respective network mask.
ip_mask	Network mask for the corresponding IP address. Use a space to separate the network mask and any subsequent IP address and network mask pairs.
tunnel	Automates the setup of IPSec tunnels specifically for management access from the corporate network to the outside interface of the ASA 5505 running as an Easy VPN Client.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called "Easy VPN Remote"). It assumes the ASA 5505 configuration contains the following commands:

vpnclient server to specify the peer.

vpnclient mode to specify the client mode (PAT) or network extension mode.

One of the following:

- **vpnclient vpngroup** to name the tunnel group and the IKE pre-shared key used for authentication on the Easy VPN server.
- **vpnclient trustpoint** to name the trustpoint identifying the RSA certificate to use for authentication

vpnclient enable to enable the ASA 5505 as an Easy VPN Client.

Note The public address of an ASA 5505 behind a NAT device is inaccessible unless you add static NAT mappings on the NAT device.

Examples

The following example shows how to generate an IPSec tunnel from the outside interface of the ASA 5505 to the host with the IP address/mask combination 192.168.10.10 255.255.255.0:

```
hostname(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
hostname(config)#
```

The following example shows how to provide management access to the outside interface of the ASA 5505 without using IPSec:

```
hostname(config)# vpnclient management clear
hostname(config)#
```

vpnclient mode

To configure the Easy VPN Remote connection for either client mode or network extension mode, use the **vpnclient mode** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

Syntax Description

client-mode	Configures the Easy VPN Remote connection to use client mode (PAT).
network-extension-mode	Configures the Easy VPN Remote connection to use network extension mode (NEM).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called "Easy VPN Remote). The Easy VPN Client supports one of two modes of operation: client mode or NEM. The mode of operation determines whether the inside hosts, relative to the Easy VPN Client, are accessible from the Enterprise network over the tunnel. Specifying a mode of operation is mandatory before making a connection because Easy VPN Client does not have a default mode.

- In client mode, the Easy VPN client performs port address translation (PAT) for all VPN traffic from its inside hosts. This mode requires no IP address management for either the inside address of the hardware client (which has a default RFC 1918 address assigned to it) or the inside hosts. Because of PAT, the inside hosts are not accessible from the enterprise network.
- In NEM, all nodes on the inside network and the inside interface are assigned addresses routable across the enterprise network. The inside hosts are accessible from the enterprise network over a tunnel. Hosts on the inside network are assigned IP addresses from an accessible subnet (statically or through DHCP). PAT is not applied to the VPN traffic when in network extension mode.

Note If the Easy VPN hardware client is using NEM and has connections to secondary servers, use the **crypto map set reverse-route** command on each headend device to configure dynamic announcements of the remote network using Reverse Route Injection (RRI).

Examples

The following example shows how to configure an Easy VPN Remote connection for client mode:

```
hostname(config)# vpnclient mode client-mode
hostname(config)#
```

The following example shows how to configure an Easy VPN Remote connection for NEM:

```
hostname(config)# vpnclient mode network-extension-mode
hostname(config)#
```

vpnclient nem-st-autoconnect

To configure the Easy VPN Remote connection to automatically initiate IPSec data tunnels when NEM and split tunneling are configured, use the **vpnclient nem-st-autoconnect** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN Client (also called “Easy VPN Remote”).

Before entering the **vpnclient nem-st-autoconnect** command, ensure that network extension mode is enabled for the hardware client. Network extension mode lets hardware clients present a single, routable network to the remote private network over the VPN tunnel. IPSec encapsulates all traffic from the private network behind the hardware client to networks behind the security appliance. PAT does not apply. Therefore, devices behind the security appliance have direct access to devices on the private network behind the hardware client over the tunnel, and only over the tunnel, and vice versa. The hardware client must initiate the tunnel. After the tunnel is up, either side can initiate data exchange.

Note You must also configure the Easy VPN server to enable network extension mode. To do so, use the **nem enable** command in group-policy configuration mode.

IPSec data tunnels are automatically initiated and sustained when in network extension mode, except when split-tunneling is configured.

Examples

The following example shows how to configure an Easy VPN Remote connection to automatically connect in network extension mode with split-tunneling configured. Network extension mode is enabled for the group policy FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

Related Commands

Command	Description
nem	Enables network extension mode for hardware clients.

vpnclient server-certificate

To configure the Easy VPN Remote connection to accept only connections to Easy VPN servers with the specific certificates specified by the certificate map, use the **vpnclient server-certificate** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

Syntax Description

certmap_name	Specifies the name of a certificate map that specifies the acceptable Easy VPN server certificate. The maximum length is 64 characters.

Defaults

Easy VPN server certificate filtering is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

Use this command to enable Easy VPN server certificate filtering. You define the certificate map itself using the crypto ca certificate map and crypto ca certificate chain commands.

Examples

The following example shows how to configure an Easy VPN Remote connection to support only connections to Easy VPN servers with the certificate map name homeservers:

```
hostname(config)# vpnclient server-certificate homeservers
hostname(config)#
```

Related Commands

Command	Description
certificate	Adds the indicated certificate.
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN Remote connection.

vpnclient server

To configure the primary and secondary IPSec servers, for the Easy VPN Remote connection, use the **vpnclient server** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient server *ip_primary_address* [*ip_secondary_address_1 ... ipsecondary_address_10*]

no vpnclient server

Syntax Description

ip_primary_address	IP address or DNS name of the primary Easy VPN (IPSec) server. Any ASA or VPN 3000 Concentrator Series can act as an Easy VPN server.
ip_secondary_address_n	(Optional) List of the IP addresses or DNS names of up to ten backup Easy VPN servers. Use a space to separate the items in the list.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

A server must be configured before a connection can be established. The **vpnclient server** command supports IPv4 addresses, the names database, or DNS names and resolves addresses in that order.

You can use either the IP address or the hostname of a server.

Examples

The following example associates the name headend-1 with the address 10.10.10.10 and uses the **vpnclient server** command to specify three servers: headend-dns.domain.com (primary), headend-1 (secondary), and 192.168.10.10 (secondary):

```
hostname(config)# names
hostname(config)# 10.10.10.10 headend-1
hostname(config)# vpnclient server headend-dns.domain.com headend-1 192.168.10.10
hostname(config)#
```

The following example shows how to configure a VPN client primary IPSec server with the IP address 10.10.10.15 and secondary servers with the IP addresses 10.10.10.30 and 192.168.10.45.

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
hostname(config)#
```

vpnclient trustpoint

To configure the RSA identity certificate to be used by the Easy VPN Remote connection, use the **vpnclient trustpoint** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient trustpoint *trustpoint_name* [**chain**]

no vpnclient trustpoint

Syntax Description

chain	Sends the entire certificate chain.
trustpoint_name	Specifies the name of a trustpoint identifying the RSA certificate to use for authentication.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505 and only when using digital certificates.

Define the trustpoint using the **crypto ca trustpoint** command. A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The commands within the trustpoint sub mode control CA-specific configuration parameters which specify how the security appliance obtains the CA certificate, how the security appliance obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

Examples

The following example shows how to configure an Easy VPN Remote connection to use the specific identity certificate named central and to send the entire certificate chain:

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters the trustpoint submode for the specified trustpoint and manages trustpoint information.

vpnclient username

To configure the VPN username and password for the Easy VPN Remote connection, use the **vpnclient username** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient username *xauth_username* **password** *xauth password*

no vpnclient username

Syntax Description

xauth_password	Specifies the password to use for XAUTH. The maximum length is 64 characters.
xauth_username	Specifies the username to use for XAUTH. The maximum length is 64 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA model 5505.

The XAUTH username and password parameters are used when secure unit authentication is disabled and the server requests XAUTH credentials. If secure unit authentication is enabled, these parameters are ignored, and the security appliance prompts the user for a username and password.

Examples

The following example shows how to configure the Easy VPN Remote connection to use the XAUTH username testuser and the password ppurkm1:

```
hostname(config)# vpnclient username testuser password ppurkm1
hostname(config)#
```

vpnclient vpngroup

To configure the VPN tunnel group name and password for the Easy VPN Remote connection, use the **vpnclient vpngroup** command in global configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpnclient vpngroup *group_name* **password** *preshared_key*

no vpnclient vpngroup

Syntax Description

group_name	Specifies the name of the VPN tunnel group configured on the Easy VPN server. The maximum length is 64 characters, and no spaces are allowed.
preshared_key	The IKE pre-shared key used for authentication by the Easy VPN server. The maximum length is 128 characters.

Defaults

If the configuration of the ASA 5505 running as an Easy VPN client does not specify a tunnel group, the client attempts to use an RSA certificate.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the ASA 5505 running as an Easy VPN client (also called “Easy VPN Remote”).

Use the pre-shared key as the password. You must configure a server before establishing a connection.

Examples

The following example shows how to configure an Easy VPN Remote connectionwith a VPN tunnel group with the group name TestGroup1 and the password my_key123.

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

Related Commands

Command	Description
vpnclient trustpoint	Configures the RSA identity certificate to be used by the Easy VPN connection.

wccp

To allocate space and to enable support of the specified Web Cache Communication Protocol (WCCP) service for participation in a service group, use the **wccp** command in global configuration mode. To disable the service group and deallocate space, use the no form of this command.

wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password]

no wccp {**web-cache** | *service-number*} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password [**0** | **7**]]

Syntax Description

web-cache	Specifies the web-cache service. **Note** Web cache counts as one service. The maximum number of services, including those assigned with the service-number argument are 256
service-number	A dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254 and up to 255. There is a maximum allowable number of 256 that includes the web-cache service specified with the **web-cache** keyword.
redirect-list	(Optional) Used with an access list that controls traffic redirected to this service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list. The access list should only contain network addresses. Port-specific entries are not supported.
access-list	Specifies the name of the access list.
group-list	(Optional) Access list that determines which web caches are allowed to participate in the service group. The access-list argument should consist of a string of no more than 64 characters (name or number) that specifies the access list.
password	(Optional) Specifies Message Digest 5 (MD5) authentication for messages received from the service group. Messages that are not accepted by the authentication are discarded.
password	Specifies the password to be used for authentication. The password argument can be up to seven characters in length.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WCCP for participation in a service group:

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password whatho
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp redirect	Enables support of WCCP redirection.

wccp redirect

To enable packet redirection on the ingress of an interface using Web Cache Communication Protocol (WCCP), use the **wccp redirect** command. To disable WCCP redirection, use the no form of this command.

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

Syntax Description

interface_name	Name of the interface where packets should be redirected..
service	Specifies the service group. You can specify the **web-cache** keyword, or you can specify the identification number (from 0 to 99) of the service.
in	Specifies redirection when packet comes into this interface

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable WCCP redirection on the inside interface for the web-cache service:

```
hostname(config)# wccp interface inside web-cache redirect in
```

Related Commands

Commands	Description
show wccp	Displays the WCCP configuration.
wccp	Enables support of WCCP with service groups.

web-agent-url

To specify the SSO server URL to which the security appliance makes SiteMinder-type SSO authentication requests, use the **web-agent-url** command in config-webvpn-sso-siteminder mode.

To remove an SSO server authentication URL, use the **no** form of this command.

web-agent-url *url*

no web-agent-url *url*

Note This command is required for SiteMinder-type SSO authentication.

Syntax Description

url	Specifies the authentication URL of the SiteMinder-type SSO server. Must contain http:// or https://.

Defaults

By default, an authentication URL is not configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn-sso-siteminder	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single-sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The SSO server has a URL that handles authentication requests.

This command applies only to the SiteMinder type of SSO server.

Use the **web-agent-url** command to configure the security appliance to send authentications to this URL. Before configuring the authentication URL, you must create the SSO server using the **sso-server** command.

For https communication between the security appliance and SSO-server, make sure that the SSL encryption settings match on both sides. On the security appliance, verify this with the **ssl encryption** command.

Examples

The following example, entered in config-webvpn-sso-siteminder mode, specifies an authentication URL of http://www.example.com/webvpn:

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
ssl encryption	Specifies the encryption algorithms the SSL/TLS protocol uses.
sso-server	Creates a single sign-on server.

web-applications

To customize the Web Application box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-applications** command from webvpn customization mode:

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the dropdown box.
text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is “Web Application”.

The default title style is background-color:#99CCCC;color:black;font-weight:bold;text-transform: uppercase

The default message text is “Enter Web Address (URL)”.

The default message style is background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is “Web Bookmarks”.

The default dropdown style is border:1px solid black;font-weight:bold;color:black;font-size:80%.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the title to “Applications”, and the color of the text to blue:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-applications title text Applications
F1-asa1(config-webvpn-custom)# web-applications title style color:blue
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

web-bookmarks

To customize the Web Bookmarks title or links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-bookmarks** command from webvpn customization mode:

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “Web Bookmarks”.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the Web Bookmarks title to “Corporate Web Bookmarks”:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.

webvpn

To enter webvpn mode, in global configuration mode, enter the **webvpn** command. To remove any commands entered with this command, use the **no webvpn** command. These webvpn commands apply to all WebVPN users.

These webvpn commands let you configure AAA servers, default group policies, default idle timeout, http and https proxies, and NBNS servers for WebVPN, as well as the appearance of WebVPN screens that end users see.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

WebVPN is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This WebVPN mode lets you configure global settings for WebVPN. WebVPN mode, which you enter from either group-policy mode or username mode, lets you customize a WebVPN configuration for specific users or group policies.

Examples

The following example shows how to enter WebVPN command mode:

```
hostname(config)# webvpn
hostname(config-webvpn)#
```

webvpn (group-policy and username modes)

To enter this webvpn mode, use the **webvpn** command in group-policy configuration mode or in username configuration mode. To remove all commands entered in webvpn mode, use the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

Webvpn commands for group policies and usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

webvpn

no webvpn

Syntax Description

This command has no arguments or keywords.

Defaults

WebVPN is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. The **webvpn** command in group-policy attributes configuration mode or username attributes configuration mode applies the settings specified in the webvpn command to the group or user specified in the parent command. In other words, webvpn mode, described in this section, and which you enter from group-policy or username mode, lets you customize a WebVPN configuration for specific users or group policies.

The webvpn attributes that you apply for a specific group policy in group-policy attributes mode override those specified in the default group policy. The WebVPN attributes that you apply for a specific user in username attributes mode override both those in the default group policy and those in the group policy to which that user belongs. Essentially, these commands let you tweak the settings that would otherwise be inherited from the default group or the specified group policy. For information about the WebVPN settings, see the description of the **webvpn** command in global configuration mode.

The following table lists the attributes you can configure in webvpn group-policy attributes and username attributes mode. See the individual command descriptions for details.

Attribute	Description
auto-signon	Configures the security appliance to automatically pass WebVPN user login credentials on to internal servers, providing a single sign-on method for WebVPN users.
customization	Specifies a preconfigured WebVPN customization to apply.
deny-message	Specifies a message to display to the user when access is denied.
filter	Identifies the access list to be used for WebVPN connections.
functions	Configures file access and file browsing, MAPI Proxy, and URL entry over WebVPN.
homepage	Sets the URL of the webpage that displays when WebVPN users log in.
html-content-filter	Identifies Java, ActiveX, images, scripts, and cookies to filter for WebVPN sessions.
http-comp	Specifies the HTTP compression algorithm to use.
keep-alive-ignore	Specifies the maximum object size to ignore for updating the session.
port-forward	Enables WebVPN application access.
port-forward-name	Configures the display name that identifies TCP port forwarding to end users.
sso-server	Configures the SSO server name.
svc	Configures SSL VPN Client attributes.
url-list	Identifies a list of servers and URLs that users can access via WebVPN.

Examples

The following example shows how to enter webvpn mode for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-webvpn)#
```

The following example shows how to enter webvpn mode for the username named "test":

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

Related Commands

clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn mode to configure webvpn attributes for the group.

show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

who

To display active Telnet administration sessions on the security appliance, use the **who** command in privileged EXEC mode.

who [*local_ip*]

Syntax Description

local_ip	(Optional) Specifies to limit the listing to one internal IP address or network address, either IPv4 or IPv6.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **who** command allows you to display the TTY_ID and IP address of each Telnet client that is currently logged into the security appliance.

Examples

This example shows the output of the **who** command when a client is logged into the security appliance through a Telnet session:

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

Related Commands

Command	Description
kill	Terminate a Telnet session.
telnet	Adds Telnet access to the security appliance console and sets the idle timeout.

window-variation

To drop a connection with a window size variation, use the **window-variation** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

Syntax Description

allow-connection	Allows the connection.
drop-connection	Drops the connection.

Defaults

The default action is to allow the connection.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **window-variation** command in tcp-map configuration mode to drop all connections with a window size that has been shrunk.

The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, “shrinking the window” is strongly discouraged. When this condition is detected, the connection can be dropped.

Examples

The following example shows how to drop all connections with a varied window size:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

```
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

wins-server

To set the IP address of the primary and secondary WINS servers, use the **wins-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a WINS server from another group policy. To prevent inheriting a server, use the **wins-server none** command.

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

Syntax Description

none	Sets wins-servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary WINS servers.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Every time you issue the **wins-server** command you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same holds true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

Examples

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

To erase the startup configuration, use the **write erase** command in privileged EXEC mode. The running configuration remains intact.

write erase

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command is not supported within a security context. Context startup configurations are identified by the **config-url** command in the system configuration. If you want to delete a context configuration, you can remove the file manually from the remote server (if specified) or clear the file from Flash memory using the **delete** command in the system execution space.

Examples

The following example erases the startup configuration:

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
delete	Removes a file from Flash memory.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

write memory

To save the running configuration to the startup configuration, use the **write memory** command in privileged EXEC mode.

write memory [**all** [**/noconfirm**]]

Syntax Description

/noconfirm	Eliminates the confirmation prompt when you use the **all** keyword.
all	From the system execution space in multiple context mode, this keyword saves all context configurations as well as the system configuration.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.2(1)	You can now save all context configurations with the **all** keyword.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line. Changes are only preserved between reboots if you save them to the startup configuration, which is the configuration loaded into running memory at startup. The location of the startup configuration for single context mode and for the system in multiple context mode can be changed from the default location (a hidden file) to a location of your choosing using the **boot config** command. For multiple context mode, a context startup configuration is at the location specified by the **config-url** command in the system configuration.

In multiple context mode, you can enter the **write memory** command in each context to save the current context configuration. To save all context configurations, enter the **write memory all** command in the system execution space. Context startup configurations can reside on external servers. In this case, the security appliance saves the configuration back to the server specified by the **config-url** command, except for HTTP and HTTPS URLs, which do not allow you to save the configuration back to the server. After the security appliance saves each context with the **write memory all** command, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

```
The context 'context a' could not be saved due to non-reachability of destination
```

- For contexts that are not saved because the context is locked, the following message appears:

```
Unable to save the configuration for the following contexts as these contexts are
locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

  A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- For contexts that are not saved because of bad sectors in the Flash memory, the following message appears:

```
The context 'context a' could not be saved due to Unknown errors
```

Because the system uses the admin context interfaces to access context startup configurations, the **write memory** command also uses the admin context interfaces. The **write net** command, however, uses the context interfaces to write a configuration to a TFTP server.

The **write memory** command is equivalent to the **copy running-config startup-config** command.

Examples

The following example saves the running configuration to the startup configuration:

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

Related Commands

Command	Description
admin-context	Sets the admin context.
configure memory	Merges the startup configuration with the running configuration.
config-url	Specifies the location of the context configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

write net

To save the running configuration to a TFTP server, use the **write net** command in privileged EXEC mode.

write net [*server***:**[*filename*] | **:***filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the security appliance treats the **tftp-server** command filename as a directory, and adds the **write net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If your TFTP server does not support this type of URL, use the **copy running-config tftp** command instead. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
*server***:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line.

In multiple context mode, this command saves only the current configuration; you cannot save all contexts with a single command. You must enter this command separately for the system and for each context. The **write net** command uses the context interfaces to write a configuration to a TFTP server. The **write memory** command, however, uses the admin context interfaces to save to the startup configuration because the system uses the admin context interfaces to access context startup configurations.

The **write net** command is equivalent to the **copy running-config tftp** command.

Examples

The following example sets the TFTP server and filename in the **tftp-server** command:

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command is not populated.

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command supplies the directory name, and the server address is overridden.

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
copy running-config tftp	Copies the running configuration to a TFTP server.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write memory	Saves the running configuration to the startup configuration.

write standby

To copy the security appliance or context running configuration to the failover standby unit, use the **write standby** command in privileged EXEC mode.

write standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You should only use this command if the configuration standby unit or failover group becomes out-of-sync with the configuration of the active unit or failover group. This typically happens when commands are entered on the standby unit or failover group.

For Active/Standby failover, the **write standby** command writes the configuration stored in the RAM of the active failover unit to the RAM on the standby unit. Use the **write standby** command if the primary and secondary unit configurations have different information. Enter this command on the active unit.

For Active/Active failover, the **write standby** command behaves as follows:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the security appliance is written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.

Note The **write standby** command replicates the configuation to the running configuration of the peer unit; it does not save the configuration to the startup configuration. To save the configuration changes to the startup configuration, use the **copy running-config startup-config** command on the same unit that you entered the **write standby** command. The command will be replicated to the peer unit and the configuration saved to the startup configuration.

When Stateful Failover is enabled, the **write standby** command also replicates state information to the standby unit after the configuration replication is complete.

Examples

The following example writes the current running configuration to the standby unit:

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

Related Commands

Command	Description
failover reload-standby	Forces the standby unit to reboot.

write terminal

To show the running configuration on the terminal, use the **write terminal** command in privileged EXEC mode.

write terminal

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This command is equivalent to the **show running-config** command.

Examples

The following example writes the running configuration to the terminal:

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

zonelabs-integrity fail-close

To configure the security appliance so that connections to VPN clients close when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command in global configuration mode.To reinstate the default whereby the VPN connections remain open on failure of the Zone Labs connection, use the **no** form of this command.

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the conncection remains open on failure.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the security appliance, the security appliance still establishes VPN client connections to the private network by default. It also maintains open, existing connections. This ensures that the enterprise VPN is not distrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command.

To return to the default condition whereby the security appliance maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command.

Examples

The following example configures the security appliance to close the VPN client connections if the Zone Labs Integrity Firewall Server fails to respond or if the connection is interrupted:

```
hostname(config)# zonelabs-integrity fail-close
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the security appliance remain open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

zonelabs-integrity fail-open

To keep remote VPN client connections to the security appliance open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command in global configuration mode. To close connections to VPN clients upon failure of the Zone Labs server connection, use the **no** form of this command.

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

Syntax Description

This command has no arguments or keywords.

Defaults

By default, remote VPN connections remain open if the security appliance does not establish or maintain a connection to the Zone Labs Integrity Firewall Server.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the primary Zone Labs Integrity Firewall Server does not respond to the security appliance, the security appliance still establishes VPN client connections to the private network by default. It also maintains existing open connections. This ensures that the enterprise VPN is not disrupted by the failure of a firewall server. If, however, you do not want the VPN connections to remain operational if the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-close** command. To then return to the default condition whereby the security appliance maintains client VPN connections if the connection to the Zone Labs Integrity Firewall Server fails, use the **zonelabs-integrity fail-open** command or the **no zonelabs-integrity fail-open** command.

Examples

The following example reinstates the default condition whereby the VPN client connections remain open if the connection to the Zone Labs Integrity Firewall Server fails:

```
hostname(config)# zonelabs-integrity fail-open
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-timeout	Specifies the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable.

zonelabs-integrity fail-timeout

To specify the time in seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Server unreachable, use the **zonelabs-integrity fail-timeout** command in global configuration mode. To restore the default timeout of 10 seconds, use the **no** form of this command without an argument.

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

Syntax Description

timeout	The number of seconds before the security appliance declares a nonresponsive Zone Labs Integrity Firewall Servers unreachable. The acceptable range is from 5 to 20 seconds.

Defaults

The default timeout value is 10 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

If the security appliance waits for the specified number of seconds without a response from the Zone Labs server, the server is declared nonresponsive. Connections to VPN clients either remain open by default or if configured to do so with the **zonelabs-integrity fail-open** command. If, however, the **zonelabs-integrity fail-close** command has been issued, the connections will close when the security appliance declares the Integrity server unresponsive.

Examples

The following example configures the security appliance to declare the active Zone Labs Intergity Server to be unreachable after 12 seconds:

```
hostname(config)# zonelabs-integrity fail-timeout 12
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-open	Specifies that VPN client connections to the security appliance remain open after the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

zonelabs-integrity interface

To specify a security appliance interface for communication with the Zone Labs Integrity Server, use the **zonelabs-integrity interface** command in global configuration mode. To reset the Zone Labs Integrity Firewall Server interface back to the default of none, use the **no** form of this command.

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

Syntax Description

interface	Specifies the security appliance interface on which the Zone Labs Integrity Firewall Server communicates. It is often an interface name created with the **nameif** command.

Defaults

By default, the Zone Labs Integrity Firewall Server interface is set to none.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example configures three Zone Labs Intergity Servers using IP addresses ranging from 10.0.0.5 to 10.0.0.7. The commands also configure the security appliance to listen to the server on port 300 and on an interface called inside:

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
hostname(config)# zonelabs-integrity port 300
hostname(config)# zonelabs-integrity interface inside
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.

Command	Description
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity port

To specify a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server, use the **zonelabs-integrity port** command in global configuration mode. To revert to the default port of 5054 for the Zone Labs Integrity Firewall Server, use the **no** form of this command.

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

Syntax Description

port	Specifies a Zone Labs Integrity Firewall Server port on the security appliance.
port_number	The number of the Zone Labs Integrity Firewall Server port. It can range from 10 to 10000.

Defaults

The default Zone Labs Integrity Firewall Server port is 5054.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance listens to the Zone Labs Integrity Firewall Server on the port and interface configured with the **zonelabs-integrity port** and **zonelabs-integrity interface** commands respectively.

Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the security appliance and then reestablish the client VPN session.

Examples

The following example configures a Zone Labs Integrity Servers using the IP address 10.0.0.5. The commands also configure the security appliance to listen to the active Zone Labs server on port 300 instead of the default 5054 port:

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
hostname(config)# zonelabs-integrity port 300
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity server-address

To add Zone Labs Integrity Firewall Servers to the security appliance configuration, use the **zonelabs-integrity server-address** command in global configuration mode. Specify the Zone Labs server by either IP address or hostname.

To remove Zone Labs Integrity Firewall Servers from the running configuration, use the **no** form of this command without arguments.

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

Note While the user interfaces appear to support the configuration of multiple Integrity Servers, the security appliance only supports one server at a time in the current release.

Syntax Description

hostname	Specifies the hostname of the Zone Labs Integrity Firewall Server. See the **name** command for hostname guidelines.
ip-address	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Command Default

By default, no Zone Labs Integrity Firewall Servers are configured.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

With this release, you can configure one Zone Labs Integrity Firewall Server. If that server fails, configure another Integrity Server first and then reestablish the client VPN session.

To specify a server by hostname, you must first configure the Zone Labs server name using the **name** command. Before using the **name** command, use the **names** command to enable it.

Note The current release of the security appliance supports one Integrity Server at a time even though the user interfaces support the configuration of up to five Integrity Servers. If the active Server fails, configure another Integrity Server on the security appliance and then reestablish the client VPN session.

Examples

The following example assigns the server name ZL-Integrity-Svr to the IP address 10.0.0.5 and configures a Zone Labs Intergity Server using that name:

```
hostname(config)# names
hostname(config)# name 10.0.0.5 ZL-Integrity-Svr
hostname(config)# zonelabs-integrity server-address ZL-Integrity-Svr
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity fail-close	Specifies that the security appliance close VPN client connections when the connection between the security appliance and the Zone Labs Integrity Firewall Server fails.
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity ssl-certificate-port

To specify a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate, use the **zonelabs-integrity ssl-certificate-port** command in global configuration mode. To revert to the default port number (80), use the **no** form of this command without an argument.

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

Syntax Description

cert-port-number	Specifies a port number on which the security appliance expects the Zone Labs Integrity Firewall Server to connect when requesting an SSL certificate.

Defaults

By default, the security appliance expects the Zone Labs Integrity Firewall Server to request an SSL certificate on port 80.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

For SSL communications between the security appliance and the Zone Labs Integrity Firewall Server, the security appliance is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (security appliance) must be authenticated by the client (Zone Labs server). The **zonelabs-integrity ssl-certificate-port** command specifies the port to which the Zone Labs server connects when requesting the SSL server certificate.

Examples

The following example configures port 30 on the security appliance to receive SSL certificate requests from the Zone Labs Integrity Server:

```
hostname(config)# zonelabs-integrity ssl-certificate-port 30
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
zonelabs-integrity ssl-client-authentication	Enables authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance.

zonelabs-integrity ssl-client-authentication

To enable authentication of the Zone Labs Integrity Firewall Server SSL certificate by the security appliance, use the **zonelabs-integrity ssl-client-authentication** command in global configuration mode with the *enable* argument. To disable authentication of the Zone Labs SSL certificate, use the *disable* argument or use the **no** form of this command without an argument.

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

Syntax Description

enable	Specifies that the security appliance authenticates the SSL certificate of the Zone Labs Integrity Firewall Server.
disable	Specifies the IP address of the Zone Labs Integrity Firewall Server.

Defaults

By default, security appliance authentication of the Zone Labs Integrity Firewall Server SSL certificate is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

For SSL communications between the security appliance and the Zone Labs Integrity Firewall Server, the security appliance is the SSL server and the Zone Labs server is the SSL client. When initiating an SSL connection, the certificate of the SSL server (security appliance) must be authenticated by the client (Zone Labs server). Authentication of the client certificate is optional, however. You use the **zonelabs-integrity ssl-client-authentication** command to enable or disable security appliance authentication of the Zone Lab server (SSL client) certificate.

Examples

The following example configures the security appliance to authenticate the SSL certificate of the Zone Labs Integrity Server:

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
hostname(config)#
```

Related Commands

Command	Description
zonelabs-integrity interface	Specifies the security appliance interface on which it communicates with the active Zone Labs Integrity Server.
zonelabs-integrity port	Specifies a port on the security appliance for communicating with a Zone Labs Integrity Firewall Server.
zonelabs-integrity server-address	Adds Zone Labs Integrity Firewall Servers to the security appliance configuration.
zonelabs-integrity ssl-certificate-port	Specifies a security appliance port to which the Zone Labs Integrity Firewall Server will connect when retrieving an SSL certificate.