



Catalyst 6500 Series and Cisco 7600 Series Switch Firewall Services Module Command Reference, 4.0

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0805R)

Catalyst 6500 Series and Cisco 7600 Series Switch Firewall Services Module Command Reference, 4.0
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



About This Guide

This preface describes who should read the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*, how it is organized, and its document conventions. This preface includes the following sections:

- [Document Objectives, page xxxiii](#)
- [Audience, page xxxiii](#)
- [Document Organization, page xxxiv](#)
- [Document Conventions, page xxxv](#)
- [Related Documentation, page xxxvi](#)
- [Obtaining Documentation, page xxxvi](#)
- [Documentation Feedback, page xxxvii](#)
- [Cisco Product Security Overview, page xxxvii](#)
- [Obtaining Technical Assistance, page xxxix](#)
- [Obtaining Additional Publications and Information, page xl](#)

Document Objectives

This guide contains the commands available for use with the FWSM to protect your network from unauthorized use.

You can also configure and monitor the FWSM 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>.

Audience

This publication is for experienced network administrators who are responsible for managing network security, configuring firewalls, managing default and static routes, and managing TCP and UDP services. Use this guide with the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

Document Organization

This guide includes the following chapters:

- Chapter 1, “Using the Command-Line Interface,” introduces you to the FWSM commands and access modes.
- Chapter 2, “aaa accounting command through accounting-server-group Commands,” provides detailed descriptions of the **aaa accounting** through **accounting-server-group** commands.
- Chapter 3, “activation-key through auto-update timeout Commands,” provides detailed descriptions of the **activation-key** through **auto-update timeout** commands.
- Chapter 4, “backup-servers through bridge-group Commands,” provides detailed descriptions of the **backup-servers** through **bridge-group** commands.
- Chapter 5, “cache-time through clear capture Commands,” provides detailed descriptions of the **cache-time** through **clear capture** commands.
- Chapter 6, “clear configure through clear configure xlate-bypass Commands,” provides detailed descriptions of the **clear configure** through **clear configure virtual** commands.
- Chapter 7, “clear console-output through clear xlate Commands,” provides detailed descriptions of the **clear console-output** through **clear xlate** commands.
- Chapter 8, “client-access-rule through curl-configure Commands,” provides detailed descriptions of the **client-access-rule** through **curl-configure** commands.
- Chapter 9, “crypto ca authenticate through crypto map set trustpoint Commands,” provides detailed descriptions of the **crypto ca authenticate** through **crypto map set trustpoint** commands.
- Chapter 10, “debug aaa through debug sip Commands,” provides detailed descriptions of the **debug aaa** through **debug sip** commands.
- Chapter 11, “default through drop Commands,” provides detailed descriptions of the **default** through **drop** commands.
- Chapter 12, “eigrp log-neighbor-changes through ftp-map Commands,” provides detailed descriptions of the **email** through **ftp-map** commands.
- Chapter 13, “gateway through http-map Commands,” provides detailed descriptions of the **gateway** through **http-map** commands.
- Chapter 14, “icmp through im Commands,” provides detailed descriptions of the **icmp** through **ignore lsamospf** commands.
- Chapter 15, “inspect ctique through inspect xdmcp Commands,” provides detailed descriptions of the **inspect ctique** through **inspect xdmcp** commands.
- Chapter 16, “interface through issuer-name Commands,” provides detailed descriptions of the **interface** through **issuer-name** commands.
- Chapter 17, “join-failover-group through kill Commands,” provides detailed descriptions of the **join-failover-group** through **kill** commands.
- Chapter 18, “ldap-base-dn through log-adj-changes Commands,” provides detailed descriptions of the **ldap-base-dn** through **log-adj-changes** commands.
- Chapter 19, “logging asdm through logout Commands,” provides detailed descriptions of the **inspect ctique** through **inspect xdmcp** commands.
- Chapter 20, “mac-address-table aging-time through multicast-routing Commands,” provides detailed descriptions of the **mac-address-table** through **multicast-routing** commands.

- Chapter 21, “name through ospf transmit-delay Commands,” provides detailed descriptions of the **name** through **ospf transmit-delay** commands.
- Chapter 22, “pager through pwd Commands,” provides detailed descriptions of the **passwd** through **pwd** commands.
- Chapter 23, “quit through rule Commands,” provides detailed descriptions of the **queue-limit** through **router-id** commands.
- Chapter 24, “same-security-traffic through show asdm sessions Commands,” provides detailed descriptions of the **same-security-traffic** through **show asdm sessions** commands.
- Chapter 25, “show asp drop through show curpriv Commands,” provides detailed descriptions of the **show asp drop** through **show curpriv** commands.
- Chapter 26, “show debug through show ipv6 traffic Commands,” provides detailed descriptions of the **show debug** through **show ipv6 traffic** commands.
- Chapter 27, “show isakmp sa through show route Commands,” provides detailed descriptions of the **show isakmp sa** through **show route** commands.
- Chapter 28, “show running-config through show running-config isakmp Commands,” provides detailed descriptions of the **show running-config** through **show running-config isakmp** commands.
- Chapter 29, “show running-config logging through show running-config xlate-bypass Commands,” provides detailed descriptions of the **show running-config logging** through **show running-config vpn-sessionb** commands.
- Chapter 30, “show service-policy through show xlate Commands,” provides detailed descriptions of the **show service-policy** through **show xlate** commands.
- Chapter 31, “shun through sysopt uauth allow-http-cache Commands,” provides detailed descriptions of the **shun** through **sysopt unauth allow-http-cache** commands.
- Chapter 32, “telnet through tunnel-limit Commands,” provides detailed descriptions of the **tcp-map** through **tunnel-limit** commands.
- Chapter 33, “upgrade-mp through xlate-bypass Commands,” provides detailed descriptions of the **upgrade-mp** through **write terminal** commands.

Document Conventions

The FWSM 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 1, “Using the Command-Line Interface.”](#)

Related Documentation

For more information, see the following documentation:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*
- *Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module to Release 3.1*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Release Notes*
- *Cisco ASDM Release Notes*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

<http://www.cisco.com/univercd/home/home.htm>

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

<http://www.cisco.com/go/marketplace/docstore>

If you do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>

To register as a Cisco.com user, go to this URL:

<http://tools.cisco.com/RPF/register/register.do>

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.



Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411

Australia: 1 800 805 227

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

<http://www.cisco.com/offer/subscribe>

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

<http://www.cisco.com/univercd/cc/td/doc/abtnicd/136957.htm>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Using the Command-Line Interface

This chapter describes how to use the CLI on the FWSM, and includes the following sections:

- [Firewall Mode and Security Context Mode, page 1-1](#)
- [Command Modes and Prompts, page 1-2](#)
- [Syntax Formatting, page 1-3](#)
- [Abbreviating Commands, page 1-3](#)
- [Command-Line Editing, page 1-3](#)
- [Command Completion, page 1-3](#)
- [Command Help, page 1-4](#)
- [Filtering show Command Output, page 1-4](#)
- [Command Output Paging, page 1-5](#)
- [Adding Comments, page 1-5](#)
- [Text Configuration Files, page 1-6](#)

**Note**

The CLI uses similar syntax and other conventions to the Cisco IOS CLI, but the FWSM 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 FWSM.

Firewall Mode and Security Context Mode

The FWSM 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 FWSM 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 FWSM 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 FWSM settings. The user EXEC mode prompt appears as follows when you first access the FWSM:

```
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 FWSM 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 1-1 **Syntax Conventions**

Convention	Description
bold	Bold text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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]} regex
```

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 *regex* with any Cisco IOS regular expression. See 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 have special meaning when used in regular expressions. [Table 1-2](#) lists the keyboard characters that have special meaning.

Table 1-2 *Using Special Characters in Regular Expressions*

Character Type	Character	Special Meaning
period	.	Matches any single character, including white space.
asterisk	*	Matches 0 or more sequences of the pattern.
plus sign	+	Matches 1 or more sequences of the pattern.
question mark	? ¹	Matches 0 or 1 occurrences of the pattern.
caret	^	Matches the beginning of the input string.
dollar sign	\$	Matches the end of the input string.
underscore	_	Matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space.
brackets	[]	Designates a range of single-character patterns.
hyphen	-	Separates the end points of a range.

1. Precede the question mark with **Ctrl-V** to prevent the question mark from being interpreted as a help command.

To use these special characters as single-character patterns, remove the special meaning by preceding each character with a backslash (\).

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 FWSM, and includes the following topics:

- [How Commands Correspond with Lines in the Text File, page 1-6](#)
- [Command-Specific Configuration Mode Commands, page 1-6](#)
- [Automatic Text Entries, page 1-6](#)
- [Line Order, page 1-7](#)
- [Commands Not Included in the Text Configuration, page 1-7](#)
- [Passwords, page 1-7](#)
- [Multiple Security Context Files, page 1-7](#)

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)# 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 FWSM, the FWSM inserts some lines automatically. For example, the FWSM 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 FWSM in their encrypted form, but you cannot unencrypt the passwords yourself.

If you enter an unencrypted password in a text file, the FWSM does not automatically encrypt them when you copy the configuration to the FWSM. The FWSM 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 FWSM, 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 command 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**] *server-tag*

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

Syntax Description

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

Defaults

The default privilege level is 0.

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
3.1(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 accounting for administrative access, use the **no** form of this command.

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

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

Syntax Description

enable	Enables accounting records to mark the entry to and exit from privileged EXEC mode.
<i>server-tag</i>	Specifies the server or group of servers to which accounting records are sent. Valid server group protocols are RADIUS and TACACS+. You must specify the name of the server group, previously specified in an aaa-server command.
ssh	Enables accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables accounting records to mark the establishment and termination of admin sessions created over Telnet. This command does not account for sessions from the switch to the FWSM (system execution space).

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced on the FWSM.
2.2(1)	This command was modified to support fallback to LOCAL.

Usage Guidelines

Sessions from the switch to the FWSM are not accounted for in the admin context, even if you have Telnet authentication enabled.

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.
	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	Removes/resets the configured AAA accounting values.
	show running-config aaa	Display the AAA configuration.

aaa accounting include, exclude

To enable accounting for connections through the FWSM, 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.
<i>inside_ip</i>	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.
<i>inside_mask</i>	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.
<i>interface_name</i>	Specifies the interface name from which users require accounting.
<i>outside_ip</i>	(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.
<i>outside_mask</i>	(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.
<i>server_tag</i>	Specifies the AAA server group defined by the aaa-server host command.
<i>service</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the FWSM. 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 FWSM 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 FWSM, 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

<i>acl_name</i>	Specifies the traffic that requires accounting by 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.
<i>interface_name</i>	Specifies the interface name from which users require accounting.
<i>server_tag</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the FWSM. 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 FWSM 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 challenge disable

To disable authentication challenge for FTP, Telnet, HTTP, or HTTPS, use the **aaa authentication challenge disable** command in global configuration mode. To reset the FWSM to default authentication, use the **no** form of this command.

aaa authentication {ftp | telnet | http | https } challenge disable

no aaa authentication {ftp | telnet | http | https } challenge disable

Syntax Description

ftp	Disables the authentication challenge for FTP connections.
http	Disables the authentication challenge for HTTP connections.
https	Disables the authentication challenge for HTTPS connections.
telnet	Disables the authentication challenge for Telnet connections.

Defaults

By default, if you enable authentication using the **aaa authentication match** or **aaa authentication [include | exclude]** commands, authentication challenge is enabled for FTP, Telnet, HTTP, and HTTPS.

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
3.1(1)	This command was introduced.

Usage Guidelines

You can configure whether the FWSM challenges users for a username and password. By default, the FWSM prompts the user when a AAA rule enforces authentication for traffic in a new session and the protocol of the traffic is FTP, Telnet, HTTP, or HTTPS. In some cases, you may want to disable the authentication challenge for one or more of these protocols. You can use the **aaa authentication challenge** command to do so.

If you disable challenge authentication for a particular protocol, traffic using that protocol is allowed only if the traffic belongs to a session previously authenticated. This authentication can be accomplished by traffic using a protocol whose authentication challenge remains enabled. For example, if you disable challenge authentication for FTP, the FWSM denies a new session using FTP if the traffic is included in an authentication rule. If the user establishes the session with a protocol whose authentication challenge is enabled (such as HTTP), FTP traffic is allowed.

Examples

The following example permits inbound access to a TCP IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command requires authentication. The authentication server is at IP address 10.16.1.20 on the inside interface. The final command disables challenge authentication for FTP, which means that users whose sessions are identified by the **aaa authentication include** command must be authenticated by Telnet, HTTP, or HTTPS, and not by FTP.

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include tcp inside 0 0 0 0 AuthIn
hostname(config)# aaa authentication ftp challenge disable
```

Related Commands

Command	Description
aaa authentication	Enables or disables authentication by including or excluding traffic.
aaa authentication match	Specifies the name of an access list, previously defined in an access-list command, that must be matched, and then provides authentication for that match.
aaa authentication secure-http-client	Provides a secure method for user authentication to the FWSM prior to allowing HTTP requests to traverse the FWSM.
aaa-server protocol	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication clear-conn

To force any active connections to close immediately after the user authentication times out or when you clear the authentication session with the **clear uauth** command, use the **aaa authentication clear-conn** command in global configuration mode. To disable this feature, use the **no** form of this command. Without this command, active connections are not terminated even though the user authentication session expired.

aaa authentication clear-conn *interface-name source_ip source_mask*

no aaa authentication clear-conn *interface-name source_ip source_mask*

Syntax Description

<i>interface-name</i>	Sets the interface name connected to the source IP address.
<i>source_ip</i>	Specifies the source IP address of the user for which you want to terminate connections.
<i>source_mask</i>	Specifies the source IP subnet mask.

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
3.2(1)	This command was introduced.

Usage Guidelines

To set the authentication timeout values, see the **timeout uauth** command.

When a connection is ended because of this command, system log message 109036 is generated.

Examples

The following example authenticates users on the inside interface from the 10.0.0.0/24 network when they access 192.168.2.0/24. These same user connections are terminated when their authentication times out.

```
hostname(config)# access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0
255.255.255.0
hostname(config)# aaa authentication mylist inside radius1
hostname(config)# aaa authentication clear-conn inside 10.0.0.0 255.255.255.0
```

Related Commands

Command	Description
aaa authentication match	Enables authentication for traffic through the FWSM.
clear configure aaa	Removes AAA configuration.
clear uauth	Clears the authentication sessions.
show running-config aaa	Displays the AAA configuration.
timeout uauth	Sets the timeout for the authentication sessions.

aaa authentication console

To authenticate users who access the FWSM CLI over an SSH, HTTP (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 {enable | telnet | ssh | http} console {LOCAL | server_group [LOCAL]}
```

```
no aaa authentication {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 FWSM 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.
	<i>server_group</i> [LOCAL]	Specifies the AAA server group tag defined by the aaa-server command. You can use a RADIUS or TACACS+ server group. If you use the LOCAL keyword in addition to the <i>server_group</i> , you can configure the FWSM 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 FWSM prompt does not give any indication which method is being used.
	ssh	Authenticates users who access the FWSM using SSH.
	telnet	Authenticates users who access the FWSM using Telnet. If you enter this command in the admin context in multiple context mode, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space). You cannot enter any AAA commands directly in the system execution space.

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 FWSM CLI with the FWSM login password (set with the **password** command). If you enter the **aaa authentication telnet console** command in the admin context in multiple context mode, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space). You cannot enter any AAA commands directly in the system execution space.

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

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

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
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support fallback to LOCAL.
3.2(1)	Support for Telnet authentication (sessioning from the switch to the FWSM) was added for the system execution space when you configure this command in the admin context.

Usage Guidelines

Before the FWSM can authenticate a Telnet or SSH user, you must first configure access to the FWSM using the **telnet** or **ssh** commands. These commands identify the IP addresses that are allowed to communicate with the FWSM. The exception is for access to the system in multiple context mode; a session from the switch to the FWSM is a Telnet session, but the **telnet** command is not required.

After you connect to the FWSM, 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 authentication according to this section, you enter the username and password as defined on the AAA server or local user database.

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 FWSM 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.

By default, you can log in to 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 HTTP authentication using this command and specify the local database, that functionality is always enabled by default. You should only configure HTTP authentication if you want to use a RADIUS or TACACS+ server for authentication. The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 16 characters.

In multiple context mode, you cannot configure any AAA commands in the system configuration. However, if you configure Telnet authentication in the admin context, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space).

As the following table shows, the action of the prompts for authenticated access to the FWSM 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
ssh	3 tries before access is denied
telnet	Continual until success
http	Continual until success

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 match	Enables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication include, exclude

To enable authentication for connections through the FWSM, 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
```

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.
<i>inside_ip</i>		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.
<i>inside_mask</i>		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.
<i>interface_name</i>		Specifies the interface name from which users require authentication.
LOCAL		Specifies the local user database.
<i>outside_ip</i>		(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.
<i>outside_mask</i>		(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.

<i>server_tag</i>	Specifies the AAA server group defined by the aaa-server command.
<i>service</i>	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 • udp/port • icmp/type • <i>protocol[/port]</i> Although you can configure the FWSM 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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

For HTTP, when you need to use a separate username and password for the AAA server and for the destination web server, use the **virtual http** command.

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 FWSM 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 FWSM 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 FWSM allows other traffic requiring authentication.

The authentication ports that the FWSM supports for AAA are fixed:

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

For Telnet and FTP, the FWSM generates an authentication prompt. After you authenticate correctly, the FWSM redirects you to your original destination. If the destination server also has its own authentication, you enter another username and password.

For HTTP, you log in using basic HTTP authentication supplied by the browser. For HTTPS, the FWSM generates custom login windows.



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 FWSM 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 FWSM username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the FWSM password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jang@jgray
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	Continual reprompting until successful login.
HTTPS	
Telnet	4 tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the FWSM checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the FWSM 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 FWSM intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the FWSM 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 FWSM sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the FWSM

If you do not want to allow HTTP(S), Telnet, or FTP through the FWSM but want to authenticate other types of traffic, you can configure virtual Telnet or virtual SSH. With virtual Telnet or SSH, the user connects using Telnet or SSH to a given IP address configured on the FWSM, and the FWSM provides a prompt. See the **virtual telnet** and **virtual ssh** commands.

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 named “tacacs+”. The second command line excludes Telnet traffic on the outside interface with a local address of 192.168.38.0, with a remote/foreign IP address of all hosts:

```
hostname(config)# aaa authentication include tcp outside 192.168.0.0 255.255.0.0 0.0.0.0
0.0.0.0 tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0
0.0.0.0 0.0.0.0 tacacs+
```

Example 2:

The following examples demonstrate ways to use the *interface-name* parameter. The FWSM 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 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

Example 3:

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

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

Example 4:

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

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

Example 5:

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

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

Example 6:

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

```
hostname(config)#aaa authentication include tcp inside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

Example 7:

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 must be authenticated by the FWSM when establishing connections through the outside interface. In this example, the first **aaa authentication** command requires authentication of all FTP, HTTP, and Telnet sessions. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. This example uses a server group named **tacacs+**.

```
hostname(config)# nat (inside) 1 10.0.0.0 255.255.255.0
hostname(config)# aaa authentication include tcp inside 0 0 tacacs+
hostname(config)# aaa authentication exclude tcp inside 10.0.0.42 255.255.255.255 tacacs+
```

Example 8:

This example permits inbound access to a TCP IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command requires authentication on HTTP. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include http inside 0 0 0 0 AuthIn
```

Related Commands

Command	Description
aaa authentication console	Enables or disables authentication on entry to privileged mode or requires authentication verification to access the FWSM via the specified type of connection.
aaa authentication match	Specifies the name of an access list, previously defined in an access-list command, that must be matched, and then provides authentication for that match.
aaa authentication secure-http-client	Provides a secure method for user authentication to the FWSM prior to allowing HTTP requests to traverse the FWSM.
aaa-server protocol	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication match

To enable authentication for connections through the FWSM, 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

<i>acl_name</i>	Specifies an extended access list name.
<i>interface_name</i>	Specifies the interface name from which to authenticate users.
LOCAL	Specifies the local user database.
<i>server_tag</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

For HTTP, when you need to use a separate username and password for the AAA server and for the destination web server, use the **virtual http** command.

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 FWSM 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 FWSM 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 FWSM allows other traffic requiring authentication.

The authentication ports that the FWSM supports for AAA are fixed:

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

For Telnet and FTP, the FWSM generates an authentication prompt. After you authenticate correctly, the FWSM redirects you to your original destination. If the destination server also has its own authentication, you enter another username and password.

For HTTP, you log in using basic HTTP authentication supplied by the browser. For HTTPS, the FWSM generates custom login windows.



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 FWSM 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 FWSM username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the FWSM password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jang@jgray
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 FWSM checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the FWSM 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 FWSM intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the FWSM 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 FWSM sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the FWSM

If you do not want to allow HTTP(S), Telnet, or FTP through the FWSM but want to authenticate other types of traffic, you can configure virtual Telnet or virtual SSH. With virtual Telnet or SSH, the user connects using Telnet or SSH to a given IP address configured on the FWSM, and the FWSM provides a prompt. See the **virtual telnet** and **virtual ssh** commands.

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 FWSM 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 or disable LOCAL or TACACS+ user authorization services.
access-list extended	Creates an access list or use a downloadable access list.

clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authentication secure-http-client

To enable SSL and secure username and password exchange between HTTP clients and the FWSM, 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 FWSM prior to allowing user HTTP-based web requests to traverse the FWSM.

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:

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

Command History	Release	Modification
	2.3(1)	This command was introduced.

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:

- A maximum of 16 concurrent HTTPS authentication processes is allowed. If all 16 HTTPS authentication processes are running, any new HTTPS connections requiring authentication are 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
```

- HTTP users see a pop-up window generated by the browser itself if **aaa authentication secure-http-client** is not configured. If **aaa authentication secure-http-client** is configured, a form loads in the browser to collect username and password. In either case, if a user enters an incorrect password, the user is reprompted. When the web server and the authentication server are on different hosts, use the **virtual** command to get the correct authentication behavior.

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 user authentication.
virtual telnet	Accesses the FWSM 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	Specifies the use of the FWSM local user database for local command authorization (using privilege levels). If LOCAL is specified 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.
<i>server_tag</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	Support added for fallback to LOCAL authorization when a TACACS+ server group is temporarily unavailable.

Usage Guidelines

You can use one of two command authorization methods:

- Local database—Configure the command privilege levels on the FWSM using the **privilege** command. When a local user authenticates with the **enable** command (or logs in with the **login** command), the FWSM places that user in the privilege level that is defined by the local database. The user can then access commands at the user privilege level and below.

You can use local command authorization without any users in the local database and without CLI or enable authentication. To do so, when you enter the **enable** command, use the system enable password, and the FWSM places you in level 15 as the default “enable_15” username. You can create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the FWSM places you in level *n*. These levels are not used unless you turn on local command authorization.

- TACACS+ server—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.

TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the FWSM 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 FWSM.

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 FWSM. 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.

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 authorization	Enables or disables user authorization.
aaa-server host	Configures host-related attributes.
aaa-server	Configures group-related server attributes.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa authorization include, exclude

To enable authorization for connections through the FWSM, 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.
<i>inside_ip</i>	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.
<i>inside_mask</i>	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.
<i>interface_name</i>	Specifies the interface name from which users require authorization.
<i>outside_ip</i>	(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.
<i>outside_mask</i>	(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.

<i>server_tag</i>	Specifies the AAA server group defined by the aaa-server command.
<i>service</i>	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]]

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM. 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 FWSM checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the FWSM sends the username to the TACACS+ server. The TACACS+ server responds to the FWSM with a permit or a deny for that traffic, based on the user profile. The FWSM 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 FWSM 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 FWSM 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	Removes/resets the configured AAA accounting values.
	show running-config aaa	Display the AAA configuration.

aaa authorization match

To enable authorization for connections through the FWSM, 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

<i>acl_name</i>	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.
<i>interface_name</i>	Specifies the interface name from which users require authentication.
<i>server_tag</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to support RADIUS servers for VPN management connection authorization.

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 FWSM 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 FWSM. 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 FWSM checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the FWSM sends the username to the TACACS+ server. The TACACS+ server responds to the FWSM with a permit or a deny for that traffic, based on the user profile. The FWSM 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 FWSM 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	Enables or disables user authorization.
clear configure aaa	Resets all aaa configuration parameters to the default values.
clear uauth	Deletes 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	Displays the AAA configuration.
show uauth	Displays 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 FWSM allows any given user account, 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

<i>number</i>	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:

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

Command History

Release	Modification
3.1(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 when the local database is used for authentication.

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

The administrator cannot be locked out of the device.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the FWSM 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 locked-out status of the user.
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 be 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 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 set 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 of 16 concurrent proxy connections per user, 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.
<i>proxy_limit</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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	Enables, disables, or views LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the aaa-server command, or ASDM user authentication.

aaa authorization	Enables or disables user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa-server host

To configure or add a AAA server to a AAA server group or 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 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 [key] [timeout seconds]
```

```
no aaa-server server_tag [(interface_name)] host server_ip [key] [timeout seconds]
```

Syntax Description

<i>(interface_name)</i>	Specifies the network interface where the authentication server resides. The parentheses are required in this parameter.
<i>key</i>	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the AAA server. Any characters entered past 127 are ignored. The key is used between the FWSM and the server for encrypting data between them. the key must be the same on both the FWSM 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 aaa-server host configuration mode.
<i>server_ip</i>	Specifies the IP address of the AAA server.
<i>server_tag</i>	Specifies the name of the AAA server group as defined by the aaa-server command. Each server group is specific to one type of server: Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.
timeout <i>seconds</i>	(Optional) Specifies the timeout interval for the request. This is the time after which the FWSM gives up on the request to the primary AAA server. If there is a standby AAA server, the FWSM 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.

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
	1.1(1)	This command was introduced.
	3.1(1)	The aaa-server command is now two separate commands: the aaa-server command adds the group and specifies the protocol while the aaa-server host command adds a server IP address to the group.

Usage Guidelines

You can have up to 15 AAA server groups in single mode or 4 AAA 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.

If accounting is in effect, the accounting information goes only to the active server, unless you specify simultaneous accounting in the **aaa-server protocol** command.

Examples

The following example configures an SDI AAA server group named “svrgrp1” on host “209.165.200.225”, 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)# aaa-server svrgrp1 host 209.165.200.225
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# sdi-version sdi-5
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands	Command	Description
	aaa-server protocol	Configures group-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.

aaa-server

To create a AAA server group and define parameters that are group-specific and common to all 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 { kerberos | ldap | nt | radius | sdi | tacacs+ }
```

```
no aaa-server server_tag protocol server-protocol
```

Syntax Description

kerberos	Specifies the Kerberos server type.
ldap	Specifies the LDAP server type.
nt	Specifies the Windows NT server type.
radius	Specifies the RADIUS server type.
sdi	Specifies the SDI server type.
<i>server_tag</i>	Specifies the name of the server group. Other AAA commands make reference to the <i>server_tag</i> group.
tacacs+	Specifies the TACACS+ server type.

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
1.1(1)	This command was introduced.
3.1(1)	Additional server types were added to RADIUS and TACACS+. The aaa-server command is now two separate commands: the aaa-server command adds the group and specifies the protocol while the aaa-server host command adds a server IP address to the group.

Usage Guidelines

Use the **aaa-server host** command to add a AAA server to the AAA server group.

You can have up to 15 AAA server groups in single mode or 4 AAA 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.

If accounting is in effect, the accounting information goes only to the active server, unless you specify simultaneous accounting in the **aaa-server protocol** command.

Examples

The following example adds a TACACS+ server group and assigns the server at 10.1.1.1 to it:

```
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  
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 10.1.1.1
```

Related Commands

Command	Description
aaa-server host	Configures parameters for specific AAA servers.
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	Specifies 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.

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

Syntax Description

<i>date</i>	Specifies the date in the format day month year; for example, 1 January 2006. The valid range of years is 1993 through 2035.
<i>time</i>	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:

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

Command History

Release	Modification
3.1(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 FWSM.
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 FWSM based on time.

accept-subordinates

To configure the FWSM 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 this 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:

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

Command History

Release	Modification
3.1(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 FWSM. 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 FWSM to accept subordinate certificates for trustpoint central:

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

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*]

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

Syntax Description

<i>access-list</i>	Access list <i>id</i> .
in	Filters the inbound packets at the specified interface.
interface <i>interface_name</i>	Name of the network interface.
out	Filters the outbound packets at the specified interface.
<i>per-user-override</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the FWSM 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 FWSM preserves the existing filtering behavior. When *per-user-override* is present, the FWSM 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.

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.

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
1.1(1)	This command was introduced.

Usage Guidelines

The **access-list alert-interval** command sets the time interval for generating the syslog message 106101. The syslog message 106101 alerts you that the FWSM has reached a deny flow maximum. When the deny flow maximum is reached, another 106101 message is generated if at least *secs* seconds have occurred since the last 106101 message.

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 FWSM.
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 commit

To commit access lists when in manual-commit mode, use the **access-list commit** command in global configuration mode.

access-list commit

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

If you set the **access-list mode** command to manual-commit, then you must manually commit access lists a before they can be used by the FWSM.



Note

Manual-commit mode only affects access lists that are not used or access lists that are used with the **access-group** command. Access lists used for other configuration commands are always committed automatically, except if the ACL mode is set to manual; then the uncommitted ACLs can not be used for the Commit feature, NAT, and AAA.

Examples

The following example shows how to commit an access list and other rules:

```
fwsM/context(config)# access-list commit
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the FWSM.

Command	Description
access-list mode	Switches the commitment mode for access lists between manual- and auto-commit.
clear access-list	Clears an access list counter.
object-group	Defines object groups that you can use to optimize your configuration.

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.

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
2.2(1)	This command was introduced.

Usage Guidelines

Syslog message 106101 is generated when the FWSM 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 used to configure policy for IP traffic through the FWSM.
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.
<i>hex_number</i>	A 16-bit hexadecimal number greater than or equal to 0x600 by which an EtherType can be identified.
<i>id</i>	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 FWSM denies all packets on the originating interface unless you specifically permit access.
- Access list logging generates syslog message 106027 for denied non-IP packets—Deny non-IP packets must be present to log denied non-IP packets.

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
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM can control any EtherType identified by a 16-bit hexadecimal number. EtherType access lists support Ethernet V2 frames. 802.3-formatted frames are not handled by the access list because they use a length field as opposed to a type field. Bridge protocol data units, which are handled by the access list, are the only exception; they are SNAP-encapsulated, and the FWSM is designed to specifically handle BPDUs.

Because EtherTypes are connectionless, you need to apply the access list 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 FWSM by configuring both MPLS routers connected to the FWSM to use the IP address on the FWSM 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 access list of each type (extended and EtherType) to each direction of an interface. You can also apply the same access lists on multiple interfaces.

**Note**

If an EtherType access list is configured to **deny all**, all ethernet frames are discarded. Only physical protocol traffic, such as auto-negotiation, for instance, 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 bpd
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 feature to act upon. To remove the 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 send 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 FWSM. 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.
<i>dest_ip</i>	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.
<i>icmp_type</i>	(Optional) If the protocol is icmp , specifies the ICMP type.
<i>id</i>	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 so you can see the access list ID better in your configuration.
inactive	(Optional) Disables an ACE. To reenble 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.
interval secs	(Optional) Specifies the log interval at which to generate a 106100 system log message. Valid values are from 1 to 600 seconds. The default is 300.

<i>level</i>	(Optional) Sets the 106100 system log message level from 0 to 7. The default level is 6.
line <i>line-num</i>	(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 deny 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 logging occurs, using system log message 106023.
<i>mask</i>	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 FWSM 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 <i>icmp_type_obj_grp_id</i>	(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 <i>network_obj_grp_id</i>	Specifies the identifier of a network object group. See the object-group network command to add an object group.
object-group <i>protocol_obj_grp_id</i>	Specifies the identifier of a protocol object group. See the object-group protocol command to add an object group.
object-group <i>service_obj_grp_id</i>	(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.
<i>operator</i>	(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 FWSM. In the case of applying application inspection to a class map (the class-map and inspect commands), this keyword applies inspection to the packet.
<i>port</i>	(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.
<i>protocol</i>	Specifies the IP protocol name or number. For example, UDP is 17, TCP is 6, and EGP is 47.

<i>src_ip</i>	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 <i>time_range_name</i>	(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 syslog 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 syslog 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM decides whether to forward or drop a packet, the FWSM tests the packet against 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 FWSM except for particular addresses, then you need to deny the particular addresses and then 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 FWSM 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 ping, specify **echo-reply (0)** (FWSM to host) or **echo (8)** (host to FWSM). 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
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 FWSM:

```
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 mode

To switch the commitment mode for access lists between manual- and auto-commit, use the **access-list mode** command in global configuration mode.

access-list mode {auto-commit | manual-commit}

Syntax Description

auto-commit	Automatically commits an access list when you add an ACE.
manual-commit	Disables auto-commit. You must manually commit an access list using the access-list commit command.

Defaults

The default is **auto-commit**.

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
2.2(1)	This command was introduced.

Usage Guidelines

When you add an ACE to an access list, the FWSM activates the access list by committing it to the network processors. In auto-commit mode, the FWSM waits a short period of time after you last entered an **access-list** command and then commits the access list. If you enter an ACE after the commitment starts, the FWSM aborts the commitment, and recommits the access list after a new short waiting period. The FWSM displays a message similar to the following after it commits the access list:

```
Access Rules Download Complete: Memory Utilization: < 1%
```

Large access lists of approximately 60 K ACEs can take 3 to 4 minutes to commit, depending on the size.

You can manually commit access lists if your management application or script needs to monitor the access list commitment for error messages. Some management applications cannot monitor errors that are the result of configuration commands, so if you add ACEs, and there is a commitment error, the management application might not receive the error. However, if the management application sets the mode to manual-commit, then it can monitor errors resulting from the **access-list commit** command, which is a run-time command. The management application typically sets this mode to manual-commit automatically.

If you enable manual commit, then you must remember to manually commit any changes you make to access lists, whether the change is an addition or a subtraction. Also, you must manually commit an access list before you assign it to an interface (**access-group** command); the FWSM cannot assign an access list to an interface if the access list does not exist yet.

If you delete an ACE, but have not yet committed your change, the **show running-config** command shows the ACE with the text “uncommitted deletion”. Adding an ACE shows the ACE as “uncommitted addition”.

**Note**

Manual-commit mode only affects access lists that are not used or access lists that are used with the **access-group** command. Access lists used for other configuration commands are always committed automatically, except if the ACL mode is set to manual; then the uncommitted ACLs can not be used for the Commit feature, NAT, and AAA.

Examples

The following example shows how to modify an existing access list using the manual-commit mode without disrupting traffic:

```
fwsM(config)# access-list mode manual-commit
fwsM(config)# clear configure access-list CHANGE ME
fwsM(config)# access-list CHANGE ME ...
! New ACE 1
fwsM(config)# access-list CHANGE ME ...
! New ACE 2
fwsM(config)# ...
fwsM(config)# access-list CHANGE ME ...
! New ACE N
fwsM(config)# access-list commit
```

The following example shows how to delete the old access list and add a new one with a different name:

```
fwsM(config)# access-list mode manual-commit
fwsM(config)# clear config access-list old-acl
fwsM(config)# access-list new-acl ... : New ACE1
fwsM(config)# access-list new-acl ... : New ACE2
fwsM(config)# .....
fwsM(config)# access-list new-acl ... : New ACEN
fwsM(config)# access-list commit
fwsM(config)# access-group new-acl in interface old-interface
```

The previous example shows that there is a slight traffic disruption on the old interface, which is equal to the time taken for the commit to complete and the **access-group** command to be applied in the last two command lines.

The following example shows how to use the manual-commit mode:

```
fwsM(config)# show access-list mode
ERROR: access-list <mode> does not exists
fwsM(config)#
fwsM(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsM(config)#
fwsM(config)# access-list 1 permit ip any any
fwsM(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsM(config)#
fwsM(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsM(config)#
```

```

fwsm(config)# access-list commit
ERROR: access-list mode set to auto-commit; command ignored
fwsm(config)#
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list mode manual-commit
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted addition)
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
ERROR: access-list not committed, ignoring command
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# no access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted deletion)
fwsm(config)#
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)# #
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#

```

Related Commands

Command	Description
access-list commit	Commits access lists when you are in manual-commit mode.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the FWSM.
clear access-list	Clears an access list counter.
show access-list	Displays the counters for an access list.
show access-list mode	Displays the compilation mode for the system.

access-list optimization enable

To optimize an access list group, use the **access-list optimization enable** command in global configuration mode. To disable this feature, use the **no** form of this command.

access-list optimization enable

no access-list optimization 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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When optimization is enabled, rules are optimized and downloaded to the NPs. The original non-optimized rules become inactive. Any addition/deletion of any rules must take place on the original non-optimized access lists. Whenever a new rule is added/deleted, the optimization process is repeated. During that processing time, some of the access lists information may not be accurate until the optimization process is complete.



Note

Access list optimization is relevant to static extended access lists only. Dynamic access lists are not optimized. In addition, when an access list is bound to AAA, policy NAT, and fixup modules, two copies of the rules coexist in the system. An optimized copy that would be used in case the access list is attached to an access group, and the original non-optimized copy used for AAA, policy NAT and fixups.

Examples

The following example shows how to optimize access lists:

```
hostname(config)# access-list optimization enable
```

Related Commands

Command	Description
clear configure access-list	Clears an access list from the running configuration.
copy optimized-running-config	Copies the optimized running configuration to the designated location.
debug acl optimization	Debugs access list optimization.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list remark

To specify the text of the 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

<i>id</i>	Name of an access list.
line <i>line-num</i>	(Optional) The line number at which to insert a remark or an access control element (ACE).
remark <i>text</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The remark text can be up to 100 characters in length, including spaces and punctuation. The remark text must contain at least 1 non-space character; you cannot enter an empty remark.

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 the 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 used to configure policy for IP traffic through the FWSM.
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. See the “Usage Guidelines” section for the description.
host <i>ip_address</i>	Specifies access to a host IP address.
<i>id</i>	Name or number of an access list.
<i>ip_address ip_mask</i>	Specifies access to a specific IP address and subnet mask.
line <i>line-num</i>	(Optional) The line number at which to insert an ACE.
permit	Permits access if the conditions are matched. See the “Usage Guidelines” section for the description.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

When you specify the *protocol* to match any Internet protocol, including TCP and UDP, use the **ip** keyword.

Refer to the **object-group** command for information on how to configure object groups.

You can use the **object-group** command to group access lists.

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. We do not recommend that you use this keyword with IPSec.

Use **host address** as an abbreviation for a mask of 255.255.255.255.

Examples

The following example shows how to deny IP traffic through the firewall:

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

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

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

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.

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 group configuration mode. To remove the accounting mode specification, use the **no** form of this command.

accounting-mode simultaneous

accounting-mode single

no accounting-mode

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:

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

Command History

Release	Modification
3.1(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
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.
aaa-server protocol	Enters AAA server group configuration mode, so that 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, in the range 1-65535, for RADIUS accounting.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the aaa-server radius-acctport command.

Usage Guidelines

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



Tip

RFC 2139 introduced a change to the standard port for RADIUS accounting, to port 1813.

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

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host “209.165.200.225”, 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 209.165.200.225
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accounting-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 that 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 tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

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

Syntax Description

server-group Specifies the name of the aaa-server group, which defaults to **NONE**.

Defaults

The default setting 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-general 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
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.



CHAPTER

3

activation-key through auto-update timeout Commands

Draft - Cisco Confidential

activation-key

To change the activation key on the FWSM and check the activation key running on the FWSM against the activation key that is stored as a hidden file in the Flash partition of the FWSM, use the **activation-key** command in global configuration mode.

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

Syntax Description

<i>activation-key-four-tuple</i>	Sets the activation key; see the “Usage Guidelines” section for formatting guidelines.
<i>activation-key-five-tuple</i>	Sets the activation key; see the “Usage Guidelines” section for formatting guidelines.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
2.2(1)	Support for 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 hexadecimal string with 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

This example shows how to change the activation key on the FWSM:

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

Related Commands

Command	Description
show activation-key	Displays the activation key.

address-pool

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

<i>address_pool</i>	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:

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

Command History

Release	Modification
3.1(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.

Examples

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

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

Related Commands

Draft - Cisco Confidential

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.

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 FWSM 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

<i>name</i>	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 FWSM 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:

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

Command History

Release	Modification
2.2(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
```

Draft - Cisco Confidential**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. 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.

alias *interface_name* *mapped_ip* *real_ip* [*netmask*]

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

Syntax Description

<i>interface_name</i>	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).
<i>mapped_ip</i>	Specifies the IP address to which you want to translate the real IP address.
<i>real_ip</i>	Specifies the real IP address.
<i>netmask</i>	(Optional) Specifies the subnet mask for both IP addresses. Enter 255.255.255.255 for a host mask.

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
Global configuration	•	—	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can also use this command to perform address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can 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 FWSM from pulling traffic toward itself via **proxy-arp** for generic NAT processing.

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

You must have an A (address) record in the DNS zone file for the “dnat” address in the **alias** command.

Draft - Cisco Confidential

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

- If the FWSM 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 FWSM gets a DNS packet that is returned to the FWSM 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.

You can 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 FWSM to be 192.168.201.29. If the FWSM uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the FWSM with SRC=209.165.201.2 and DST=192.168.201.29. The FWSM translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

This 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 FWSM because the client assumes that the 209.165.201.29 is on the local inside network.

To correct this, 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 FWSM 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.

Draft - Cisco Confidential

allocate-acl-partition

To assign a context to a memory partition, use the **allocate-acl-partition** command in context configuration mode. To remove the assignment, use the **no** form of this command.

allocate-acl-partition *partition_number*

no allocate-acl-partition *partition_number*

Syntax Description

<i>partition_number</i>	Specifies the partition number as an integer from 0 to the number of partitions available, minus 1. The default is 12 partitions, so the range is 0 to 11. See the resource acl-partition command to configure the number of memory partitions.

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
Context configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.3(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. By default, a context belongs to one of 12 partitions that offers a maximum of 12,130 rules, including ACEs, AAA rules, and others. The FWSM assigns contexts to the partitions in the order they are loaded at startup. For example, if you have 12 contexts, each context is assigned to its own partition, and can use 12,130 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to partition 1, and can use 12,130 rules divided between them; the other 11 contexts continue to use 12,130 rules each. If you delete contexts, the partition membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.

**Note**

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

Alternatively, you can manually assign a context to a partition with the **allocate-acl-partition** command. You can also reduce the number of partitions to better match the number of contexts you have with the **resource acl-partition** command.

When you assign a context to a partition, then the partition becomes *exclusive*. An exclusive partition only includes contexts that you specifically assign to it. Partitions that do not have contexts specifically assigned to them are non-exclusive and contexts are allocated to them in a round-robin fashion.

**Note**

If you assign contexts to all partitions, then they are all exclusive. If you later add a context that is not assigned to a partition, however, then it is assigned to partition 0 by default.

Examples

The following example assigns context test to partition 0:

```
hostname# context test
hostname(config-ctx)# allocate-acl-partition 0
```

Related Commands

Command	Description
context	Configures a security context.
resource acl-partition	Determines the number of memory partitions for multiple context mode.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.

Draft - Cisco Confidential

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 *vlannumber*[-*vlannumber*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *vlannumber*[-*vlannumber*]

Syntax Description	
invisible	(Default) Allows context users to only see the mapped name (if configured) in the show interface command.
<i>map_name</i>	(Optional) Sets a mapped name. The <i>map_name</i> is an alphanumeric alias for the interface that can be used within the context instead of the VLAN ID. If you do not specify a mapped name, the VLAN 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. You can use the same name in multiple contexts; the VLAN ID in multiple contexts can be the same or different for a given name. You cannot use the same name for different VLAN IDs in the same 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: <pre>int0 inta int_0</pre> You can specify a range of mapped names. See the “Usage Guidelines” section for more information about ranges.
visible	(Optional) Allows context users to see physical interface properties in the show interface command even if you set a mapped name.
<i>vlannumber</i>	Sets the VLAN number, typically from 2 to 1000 and from 1025 to 4094 (see the switch documentation for supported VLANs). To view all interfaces currently configured on the FWSM, enter the show running-config interface command or the show interface command. You can only allocate an interface that exists in the system configuration. By default, all VLANs assigned to the FWSM by the switch are added to the system configuration. You can also add VLANs manually to the system configuration, but you need to assign them from the switch if you want them to pass traffic.

Defaults

The VLAN 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:

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

Command History

Release	Modification
2.2(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 VLAN 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 FWSM removes any interface-related configuration in the context.

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 VLAN IDs, 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
```

- The numeric portion of the mapped name must include the same quantity of numbers as the **vlanx-vlany** statement. For example, both ranges include 100 interfaces:

```
vlan100-vlan199 int1-int100
```

If you enter **vlan100-vlan199 int1-int15** or **vlan100-vlan199 happy1-sad5**, for example, the command fails.

Examples

The following example shows VLANs 100, 200, and 300 through 305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx) # allocate-interface vlan100 int1
hostname(config-ctx) # allocate-interface vlan200 int2
hostname(config-ctx) # allocate-interface vlan300-vlan305 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.

Draft - Cisco Confidential

Command	Description
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.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Draft - Cisco Confidential

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

<i>area_id</i>	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 <i>area_id</i> .

Defaults

Area authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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

Draft - Cisco Confidential

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

<i>area_id</i>	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.
<i>cost</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Draft - Cisco Confidential

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

<i>area_id</i>	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.
<i>list_name</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

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)#
```

Draft - Cisco Confidential**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

<i>area_id</i>	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 <i>metric_value</i>	(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:

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

Draft - Cisco Confidential**Command History**

Release	Modification
1.1(1)	This command was introduced.

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

<i>address</i>	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates type 3 summary link-state advertisements (LSAs).
<i>area_id</i>	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.
<i>mask</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Draft - Cisco Confidential**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

<i>area_id</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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)#
```

Draft - Cisco Confidential

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

<i>area_id</i>	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 <i>key</i>	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval <i>seconds</i>	(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 <i>seconds</i>	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 <i>key</i>	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key <i>key_id</i>	(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 <i>seconds</i>	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
<i>router_id</i>	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 <i>seconds</i>	(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.

Draft - Cisco Confidential

- **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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Draft - Cisco Confidential**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 FWSM receives an ARP request for the specified IP address, then it responds with the FWSM MAC address. When the FWSM receives traffic destined for the host belonging to the IP address, the FWSM 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 FWSM does not perform proxy ARP.
<i>interface_name</i>	The interface attached to the host network.
<i>ip_address</i>	The host IP address.
<i>mac_address</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM, 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 FWSM 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.

Draft - Cisco Confidential

arp timeout

To set the time before the FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example changes the ARP timeout to 5000 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 FWSM drops the packet.
<i>interface_name</i>	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 FWSM. 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:

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

Command History

Release	Modification
2.2(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 FWSM 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 FWSM drops the packet.

Draft - Cisco Confidential

- If the ARP packet does not match any entries in the static ARP table, then you can set the FWSM to either forward the packet out all interfaces (flood), or to drop the packet.

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 FWSM, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the FWSM 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

<i>session</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm disconnect command).
3.1(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
```

Draft - Cisco Confidential

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:

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

Command History

Release	Modification
3.1(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 FWSM. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, and the associated log sessions, 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.

Draft - Cisco Confidential**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

<i>real_grp_name</i>	The name of an ASDM object group.
<i>real_if_name</i>	The name of the interface to which the specified object group is associated.
<i>ref_grp_name</i>	The name of an object group that contains translated IP addresses of the object group specified by the <i>real_grp_name</i> argument.
<i>ref_if_name</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm group command).
3.1(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.

Draft - Cisco Confidential

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm history enable command).
3.1(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 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

<i>ip_addr</i>	IP address used internally by ASDM to define the network topology.
<i>netmask</i>	The subnet mask for <i>ip_addr</i> .
<i>if_name</i>	The name of the interface through which ASDM is accessed.
<i>ipv6_addr/prefix</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as the pdm location command).
3.1(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.

Draft - Cisco Confidential

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

In some situations, return traffic for a session may be routed through a different interface than it originated from. In failover configurations, return traffic for a connection that originated on one unit may return through the peer unit. This most commonly occurs when two interfaces on a single FWSM, or two FWSMs in a failover pair, are connected to different service providers and the outbound connection does not use a NAT address. By default, FWSM drops the return traffic because there is no connection information for the traffic.

You can prevent the return traffic from being dropped using the **asr-group** command on interfaces where this is likely to occur. When an interface configured with the **asr-group** command receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same group.

**Note**

In failover configurations, you must enable Stateful Failover for session information to be passed from the standby unit or failover group to the active unit or failover group.

If it does not find a match, the packet is dropped. If it finds a match, then one of the following actions occurs:

- If the incoming traffic originated on a peer unit in a failover configuration, some or all of the layer 2 header is rewritten and the packet is redirected to the other unit. This redirection continues as long as the session is active.
- If the incoming traffic originated on a different interface on the same unit, some or all of the layer 2 header is rewritten and the packet is reinjected into the stream.

**Note**

Using the **asr-group** command to configure asymmetric routing support is more secure than using the **static** command with the **nailed** option.

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 Vlan101
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 Vlan102
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.

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

<i>as-number</i>	The autonomous system number of the EIGRP process being authenticated. This must be the same values as configured for the EIGRP routing process.
<i>key</i>	Key to authenticate EIGRP updates. The key can contain up to 16 characters.
key-id <i>key-id</i>	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:

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

Command History

Release	Modification
4.0(1)	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 vlan10:

```
hostname(config)# interface vlan10
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.

Draft - Cisco Confidential

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

<i>as-num</i>	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:

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

Command History

Release	Modification
4.0(1)	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 vlan10:

```
hostname(config)# interface vlan10
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-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-port** command in AAA-server host 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the aaa-server radius-authport command.

Usage Guidelines

If your RADIUS authentication server uses a port other than 1645, you must configure the FWSM for the appropriate port prior to starting the RADIUS service with the **aaa-server** command.



Tip

RFC 2138 introduced a change to the standard port for RADIUS authentication, to port 1812.

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

Examples

The following example configures a RADIUS 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 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
```

Draft - Cisco Confidential

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 that 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

To specify the aaa-server group to use for user authentication, use the **authentication-server-group** command in tunnel-group general-attributes mode. To return this command 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

<i>interface name</i>	(Optional) Specifies the interface the IPSec tunnel terminates.
LOCAL	(Optional) Specifies authentication to be performed 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. To indicate that authentication is not required, use the NONE keyword as the server group name.
<i>server group</i>	Specifies the name of the aaa-server group, which defaults to LOCAL .

Defaults

The default setting for this command is **LOCAL**.

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
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to the IPSec remote access tunnel-group type only:

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
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)#
```

Draft - Cisco Confidential

Related Commands	Command	Description
	aaa-server host	Configures 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.
	tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-dn-attributes

To specify what part of the subject DN field to use as the username for authorization, use the **authorization-dn-attributes** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

[no] authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

Syntax Description

<i>primary-attr</i>	Specifies the attribute to use in deriving a name for an authorization query from a certificate.
<i>secondary-attr</i>	(Optional) Specifies an additional attribute to use in deriving a name for an authorization query from a certificate, if the primary attribute does not exist.
use-entire-name	Specifies that the FWSM should use the entire subject DN (RFC 1779) to derive the name.

Defaults

The default value for the primary attribute is Common Name.

The default value for the secondary attribute is Organization Unit.

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
Tunnel-group ipsec-attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote access tunnel type only.

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

Draft - Cisco Confidential

Attribute	Definition
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

Examples

The following example entered in config-ipsec configuration mode, creates a remote access tunnel group (ipsec_ra) named remotegrp, specifies IPSec group attributes and defines the Common Name to be used as the username for authorization:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-ipsec)#
```

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-required

To require users to authorize successfully to connect, use the **authorization-required** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

[no] authorization-required

Defaults

The default setting of this command is disabled.

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
Tunnel-group general attributes configuration	•	•	•	•	—

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only.

Examples

The following example entered in config-ipsec 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 ipsec-attributes mode for the specified tunnel group, and the last command specifies authorization required for the named tunnel group:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-required
hostname(config-ipsec)#
```

Draft - Cisco Confidential

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

authorization-server-group

To specify the aaa-server group for user authorization, use the **authorization-server-group** command in tunnel-group general-attributes mode. To return this command to the default, use the **no** form of this command.

authorization-server-group *server group*

no authorization-server-group

Syntax Description

server group Specifies the name of the aaa-server group, which defaults to **none**.

Defaults

The default setting for this command is **no authorization-server-group**.

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
Tunnel-group general-attributes	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to IPSec remote access tunnel-group types.

When VPN Authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

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
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

Related Commands

Command	Description
aaa-server host	Configures AAA-server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.

Draft - Cisco Confidential

Command	Description
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.

auth-prompt

To specify or change the AAA challenge text for through-the-FWSM 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** | **accept** | **reject** [**invalid-credentials** | **expired-pwd**] } *string*

no auth-prompt { **prompt** | **accept** | **reject** [**invalid-credentials** | **expired-pwd**] }

Syntax Description

accept	Sets the text that displays when a user authentication is accepted.
expired-pwd	(Optional) Sets the text that displays when a user authentication is rejected due to an expired password. This prompt is only used if the RADIUS server uses a Windows Active Directory server for the username and password. You must configure a prompt using the expired-pwd keyword for the user to be prompted for a new password.
invalid-credentials	(Optional) Sets the text that displays when a user authentication is rejected due to invalid credentials, such as an incorrect username or password.
prompt	Sets the AAA challenge prompt for username and password.
reject	Sets the text that displays when a user authentication is rejected. When you enter the reject keyword without the invalid-credentials or reject expired-pwd keywords, then this generic prompt is displayed for all rejections that are not due to invalid credentials or expired passwords. For a rejection due to an invalid credential or an expired password, then the prompt you set for the invalid-credentials or reject expired-pwd keyword displays. If you do not set any prompts for invalid credentials or expired passwords, then the generic reject prompt is shown in all cases.
<i>string</i>	Sets 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, the prompt users see when they log in depends on the protocol they use:

- Users who log in using HTTP see the following prompt: `HTTP Authentication.`
- Users who log in using FTP see the following prompt: `FTP Authentication.`
- Users who log in using Telnet see no prompt.

Draft - Cisco Confidential**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
1.1(1)	This command was introduced.
3.2(1)	The expired-pwd and invalid-credentials keywords were added.

Usage Guidelines

The **auth-prompt** command lets you specify the AAA challenge text for HTTP, HTTPS, FTP, and Telnet access through the FWSM 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 (the **prompt** keyword), or after the user enters the username and password (the **accept** and **reject** keywords).

**Note**

Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and 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:
```

You can also provide separate messages to display when the FWSM accepts or rejects the authentication attempt; for example:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

To set rejection messages for invalid credentials, expired password, and for unknown rejection reasons, enter the following commands:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt reject invalid-credentials Incorrect username or password
hostname(config)# auth-prompt reject expired-pwd Your password is expired. Reset your
password and try again.
```

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.

Draft - Cisco Confidential

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 EIGRP.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Route summarization reduces the amount of routing information in the routing tables. 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 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.

Command	Description
router eigrp	Enables the EIGRP routing process and enters EIGRP router configuration mode.
show running-config router	Displays the router commands and router configuration mode commands in the running configuration.

Draft - Cisco Confidential

auto-update device-id

To configure the FWSM 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 FWSM to uniquely identify the device.
hostname	Uses the hostname of the FWSM to uniquely identify the device.
ipaddress <i>[if_name]</i>	Uses the IP address of the FWSM to uniquely identify the FWSM. By default, the FWSM uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the <i>if_name</i> .
mac-address <i>[if_name]</i>	Uses the MAC address of the FWSM to uniquely identify the FWSM. By default, the FWSM 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 <i>if_name</i> .
string <i>text</i>	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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM 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.

Draft - Cisco Confidential

auto-update poll-period

To configure how often the FWSM 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

<i>poll_period</i>	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
<i>retry_count</i>	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
<i>retry_period</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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 FWSM 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.

Draft - Cisco Confidential

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 FWSM periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

auto-update server *url* [*verify-certificate*]

no auto-update server *url* [*verify-certificate*]

Syntax Description

<i>url</i>	Specifies the location of the Auto Update Server using the following syntax: http[s]:[[user:password@]location [:port]] / pathname
<i>verify_certificate</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Only one server can be configured.

Examples

The following example sets the Auto Update Server URL:

```
hostname(config)# auto-update server http://10.1.1.1:1741/
```

Related Commands

auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the FWSM checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the FWSM 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.

Draft - Cisco Confidential

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 FWSM stops all traffic through the FWSM. Set a timeout to ensure that the FWSM 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 FWSM to never time out.

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
3.1(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 FWSM device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the FWSM 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.

Draft - Cisco Confidential



CHAPTER

4

backup-servers through bridge-group Commands

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 FWSM is unavailable. When you configure backup servers, the FWSM 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 FWSM pushes a null server list.
keep-client-config	Specifies that the FWSM sends no backup server information to the client. The client uses its own backup server list, if configured.
<i>server1 server 2.... server10</i>	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary FWSM 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 FWSM.

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
Group-policy	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Configure backup servers either on the client or on the primary FWSM. If you configure backup servers on the FWSM, 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 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 {**exec** | **login** | **motd** *text*}

[**no**] **banner** {**exec** | **login** | **motd** [*text*]}

Syntax Description

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 FWSM using Telnet.
motd	Configures the system to display a message-of-the-day banner.
<i>text</i>	Line of message text to display.

Defaults

The default is no login, session, or message-of-the-day banner.

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
2.2(1)	This command was introduced.

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 FWSM. 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 FWSM 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 FWSM 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

The following example shows how to configure the **exec**, **login**, and **motd** banners:

```
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
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
```

The following 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
```

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 <i>banner_string</i>	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:

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

Command History

Release	Modification
3.1(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
    
```


bgp router-id

To specify a router ID for BGP routing process on the FWSM, use the **bgp router-id** command in router configuration mode. To restore the default router ID, use the **no** form of this command.

bgp router-id *ip-addr*

no bgp router-id *ip-addr*

Syntax Description

<i>ip-addr</i>	An IP address. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the FWSM.

Defaults

The router ID is set to the highest IP address configured on the FWSM.

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 ¹	System
Router configuration	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

Use the **bgp router-id** command to configure a fixed router ID for a local BGP routing process. Enter the router ID in IP address format. You can use any valid IP address, even an address that is not locally configured on the FWSM. Changing the router ID causes peering sessions to automatically reset.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example shows a BGP routing configuration with the router ID of the FWSM set to 192.168.1.1:

```
hostname(config)# router bgp 800
hostname(config-router)# bgp router-id 192.168.1.1
hostname(config-router)# neighbor 10.1.1.1 remote-as 800
hostname(config-router)# neighbor 10.1.1.1 password bQ2$F78t
hostname(config-router)# network 192.168.1.0 mask 255.255.255.0
hostname(config-router)# network 10.1.1.0 mask 255.255.255.0
```

Related Commands	Command	Description
	router bgp	Creates a BGP routing process and enters router configuration mode for that process.
	show running-config router	Displays the router commands in the running configuration.

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

<i>memory_size</i>	(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:

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

Command History

Release	Modification
7.0(1)	Support for this command was introduced.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.
If you reload the FWSM, 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 device (IOS)

By default, the FWSM boots from the **cf:4** application partition. However, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. To change the default boot partition, enter the **boot device** command in global configuration mode. To restore the default, use the **no** form of this command.

boot device module *mod_num* **cf:n**

no boot device module *mod_num* [**cf:n**]

Syntax Description	cf:n	Sets the boot partition. Application partitions include cf:4 (the default) and cf:5 . The maintenance partition is cf:1 .
	module <i>mod_num</i>	Specifies the module number. Use the show module command to view installed modules and their numbers.

Defaults The default boot partition is cf:4.

Command Modes Global configuration.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines To view the current boot partition, enter the **show boot device** command:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Examples The following example shows how to set the boot partition to the maintenance partition:

```
Router(config)# boot device module 1 cf:1
```

Related Commands

Command	Description
hw-module module reset	Resets the module.
show boot device	Shows the boot partitions of each module.
show module	Shows all installed modules.

bridge-group

To assign an interface to a bridge group in transparent firewall mode, use the **bridge-group** command in interface configuration mode. To unassign an interface, use the **no** form of this command. A transparent firewall connects the same network on its inside and outside interfaces. Each pair of interfaces belongs to a bridge group.

bridge-group *number*

no bridge-group *number*

Syntax Description

number Specifies an integer between 1 and 100.

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
Interface configuration	—	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can configure up to eight bridge groups of two interfaces each. You can only assign two interfaces to a bridge group. You cannot assign the same interface to more than one bridge group.

Assign a management IP address to the bridge group using the **interface bvi** command and then the **ip address** command.

Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Examples

The following example assigns VLAN 100 to bridge group 1:

```
hostname(config)# interface vlan 100
```

```
hostname(config-if)# bridge-group 1
```

Related Commands

Command	Description
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.
nameif	Sets the interface name.
security-level	Sets the interface security level.



CHAPTER

5

cache-time through clear capture Commands

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 ca-crl 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		
	Routed	Transparent	Single	Multiple Context	System
Ca-crl configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	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

<i>ip_address</i>	The IP address of the gateway.
<i>group_id</i>	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:

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

Command History

Release	Modification
3.1(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.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command. To disable packet capture capabilities, use the **no** form of this command.

```
capture capture_name [type {asp-drop [drop-code] | raw-data | isakmp}]
    access-list access_list_name interface interface_name [buffer buf_size] [ethernet-type type]
    [packet-length bytes] [circular-buffer]
```

```
no capture capture-name [type {asp-drop [drop-code] | raw-data | isakmp}] [access-list
    access_list_name] [interface interface_name]
```

Syntax Description

access-list <i>access_list_name</i>	Captures traffic that matches an access list. In multiple context mode, this is only available within a context. This keyword is required except when you specify type asp-drop .
asp-drop <i>drop-code</i>	(Optional) Captures packets dropped by the accelerated security path. The <i>drop-code</i> 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 <i>drop-code</i> argument, then all dropped packets are captured. You can enter this keyword with packet-length , circular-buffer , and buffer , but not with interface , access-list or ethernet .
buffer <i>buf_size</i>	(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops.
<i>capture_name</i>	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.
ethernet-type <i>type</i>	(Optional) Selects an Ethernet type to capture. The default is IP packets.
interface <i>interface_name</i>	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. This keyword is required except when you specify type asp-drop .
isakmp	(Optional) Captures ISAKMP traffic. In multiple context mode, this is only available within a context.
packet-length <i>bytes</i>	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces. This setting is the default.
type	(Optional) Lets you specify the type of data captured.

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 68 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
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	Added the capability to capture all traffic, not just traffic that passes through the general-purpose processor.

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.

The FWSM is capable of tracking all IP traffic that flows across it. It is also capable of capturing all the IP traffic that is destined to the FWSM, including all the management traffic (such as SSH and Telnet traffic) to the FWSM.

Enter the **no capture** command with the **access-list** and **interface** keywords to stop the capture without deleting the capture buffer. To stop the capture and delete the buffer, enter **no capture name** without additional keywords.



Note

The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby unit during failover.

Examples

This example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
hostname(config)# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname(config)# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname(config)# capture captest access-list http packet-length 74 interface inside
```

On a web browser, the capture contents for a capture named “captest” can be viewed at the following location:

https://171.69.38.95/capture/captest/pcap

To download a libpcap file (used in web browsers such as Internet Explorer or Netscape Navigator) to a local machine, enter the following:

https://171.69.38.95/capture/http/pcap

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 [**flash:**] *[path]*

Syntax Description

flash:	Specifies the internal Flash memory, followed by a colon.
<i>path</i>	(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:

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

Command History

Release	Modification
2.2(1)	Support for 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.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain mode. When you use this command, the FWSM 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 the command.

certificate {**ca** | **ra-encrypt** | **ra-sign** | **ra-general**} *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

<i>certificate-serial-number</i>	Specifies the serial number of the certificate in hexadecimal format ending with the word quit.
ca	Indicates that the certificate is a certificate authority issuing certificate.
ra-encrypt	Indicates that the certificate is a registration authority key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is a registration authority certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an registration authority digital signature certificate used in SCEP messaging.

Defaults

This command has no default 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 chain configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A certificate authority 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 registration authority to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

Examples

This example enters ca trustpoint mode for a trustpoint named central, then enters crypto ca certificate chain mode for central, and 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

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-ipsec 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-ipsec)# chain
hostname(config-ipsec)#
```

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto {**system** | **context** *name*}

Syntax Description

context <i>name</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

If you log in to 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 mode, 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.

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 FWSM checks the entire heap, validating each memory buffer. If there is a discrepancy, the FWSM issues either an “allocated buffer error” or a “free buffer error.” If there is an error, the FWSM dumps traceback information when possible and reloads.
validate-checksum		Sets the code space checksum validation interval. When the FWSM first boots up, the FWSM calculates a hash of the entire code. Later, during the periodic check, the FWSM generates a new hash and compares it to the original. If there is a mismatch, the FWSM issues a “text checksum checkheaps error.” If there is an error, the FWSM dumps traceback information when possible and reloads.
<i>seconds</i>		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:

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

Command History	Release	Modification
	3.1(1)	Support for 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
```

■ checkheaps

Related Commands

Command	Description
show checkheaps	Shows checkheaps statistics.

class

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

<i>name</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the FWSM, 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 FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.



Note

The FWSM does not limit the bandwidth per context; however, the switch containing the FWSM can limit bandwidth per VLAN. See the switch documentation for more information.

When you create a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM 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 a 2 percent limit 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.
- IPsec 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 with all resources set to 5 percent, except for fixups, with a setting of 10 percent, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

To add a class called silver with all resources set to 3 percent, except for system log messages, with a setting of 500 per second, enter the following commands:

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

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** 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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. This is for internal use only, and cannot be modified.

Including the class-default class map, up to 63 **class** and **match** commands can be configured in a policy map.

After you add the class map to the policy map with the **class** command, you can define one or more actions to be performed on the traffic. Features supported in class configuration mode of a Layer 3/4 policy map include:

- Connection features
- Application inspection

Features supported in class configuration mode of an inspection policy map include:

- Dropping a packet
- Dropping a connection

- Resetting a connection
- Logging
- Masking content

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 FWSM 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

<i>class_map_name</i>	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 reuse 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
3.1(1)	This command was introduced.

Usage Guidelines

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. This is for internal use only, and cannot be modified.

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. The configuration includes a default Layer 3/4 class map that the FWSM 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
```

You can create multiple Layer 3/4 class maps 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** 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 that identifies the traffic included in the class map except if you have the **match default-inspection-traffic** command. In that case, you can specify a **match access-list** command along with the **match default-inspection-traffic** command to narrow the matched traffic. Because the **match default-inspection-traffic** command specifies the ports to match, any ports in the access list are ignored.

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
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**] *class_map_name*

no class-map [**type inspect** *application* [**match-all**]] *class_map_name*

Syntax Description

<i>application</i>	Specifies the type of application traffic you want to match. Available types include: http sip
<i>class_map_name</i>	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 reuse 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 and only option.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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. 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 HTTP traffic, you can match text in a URL.

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.

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
```

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

<i>class_map_name</i>	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 reuse 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:

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

Command History

Release	Modification
4.0(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.

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 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.
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 a user 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.
<i>name</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use this command when a user fails authentication a few times, but you want to reset the counter to zero, for example, when the configuration has recently been modified.

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 FWSM reboots.

Locking or unlocking a username results in a syslog 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 a user locked-out status.
show aaa local user [locked]	Shows the list of usernames that are currently locked.

clear aaa local user logout

To clear the logout status of the specified users and set their failed-attempts counter to 0, use the **clear aaa local user logout** command in privileged EXEC mode.

clear aaa local user logout {*username name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
<i>name</i>	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:

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

Command History

Release	Modification
3.1(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 logout** command to clear the logout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user logout 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 user's locked-out status.
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 privileged EXEC mode.

```
clear aaa-server statistics [LOCAL | groupname [host hostname] | protocol protocol]
```

Syntax Description	LOCAL	(Optional) Clears statistics for the LOCAL user database.
	<i>groupname</i>	(Optional) Clears statistics for servers in a group.
	host <i>hostname</i>	(Optional) Clears statistics for a particular server in the group.
	protocol <i>protocol</i>	(Optional) Clears statistics for servers of the specified 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:					
	Command Mode	Firewall Mode		Security Context		
		Routed	Transparent	Single	Multiple	
					Context	System
	Privileged EXEC	•	•	•	•	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

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 configuration mode.

clear access-list [*id*] **counters**

Syntax Description

counters	Clears access list counters.
<i>id</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.
<i>type</i>	(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:

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

Command History

Release	Modification
3.1(1)	Support for 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-ooout
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 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:

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

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines Resets the low watermark counters to the current available blocks in each pool. Also clears the history information stored during the last buffer allocation failure.

Examples The following example clears the blocks:

```
hostname# clear blocks
```

Command	Description
blocks	Increases the memory assigned to block diagnostics
show blocks	Shows the system buffer utilization.

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command.

clear capture *capture_name*

Syntax Description

capture_name Name of the packet capture.

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
Privileged Mode	•	•	•	•	•

Command History

Release	Modification
2.2(1)	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 “trudy”:

```
hostname(config)# clear capture trudy
```

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.



CHAPTER

6

clear configure through clear configure xlate-bypass 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

<i>command</i>	Clears the configuration for a specified command. For more information, see individual entries in this guide for each clear configure <i>command</i> 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).
all	Clears the entire running configuration.

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
1.1(1)	This command was introduced.
3.1(1)	This command was modified to allow you to clear the configuration for each command.

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.
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:

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

Command History

Release	Modification
1.1(1)	The clear aaa command was introduced.
3.1(1)	This command was changed from clear aaa .

Usage Guidelines

This command also resets the AAA parameters to their default values, if any.

Examples

```
hostname(config)# clear configure aaa
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting.
aaa authentication	Enables or disables user authentication.
aaa authorization	Enables or disables user authorization.
show running-config aaa	Displays 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

<i>server-ip</i>	The IP address of the AAA server.
<i>server-tag</i>	(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:

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

Command History

Release	Modification
1.1(1)	The clear aaa-server command was introduced.
3.1(1)	This command was changed from clear aaa-server .

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

Given the following configuration:

```
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
```

several commands and examples follow.

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	Lets you configure AAA server parameters that are group-specific and common to all hosts.
show running-config aaa	Displays 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.

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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from clear access-group .

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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.
show access-list	Displays counters for an access list.
show running-config access-list	Displays the access list configuration running on the FWSM.

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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from clear alias .

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:

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

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	The configure keyword was added.

Examples The following example clears static ARP entries from the configuration:

```
hostname# 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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	This command was changed from clear arp-inspection .

Examples The following example clears the ARP inspection configuration:

```
hostname# 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**]

Syntax Description

group	(Optional) Clears only the asdm group commands 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as the clear pdm command).
3.1(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 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 FWSMs running in multiple context mode, 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 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:

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

Command History

Release	Modification
1.1(1)	The clear auth-prompt command was introduced.
3.1(1)	This command was changed from clear auth-prompt .

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 the following prompt: `HTTP Authentication`.
- Users who log in using FTP see the following prompt: `FTP Authentication`.
- Users who log in using Telnet see no prompt.

Examples

The following 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 auto-update

To clear the Auto Update Server configuration, use the **clear configure auto-update** command in global configuration mode.

clear configure auto-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:

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

Release	Modification
3.1(1)	This command was introduced.

Examples The following example clears the ARP inspection configuration:

```
hostname# clear configure auto-update
```

Related Commands	Command	Description
	auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
	auto-update poll-period	Sets how often the FWSM 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 FWSM if the Auto Update Server is not contacted within the timeout period.
	show running-config auto-update	Shows the Auto Update Server configuration.

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:

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

Release	Modification
2.2(1)	The clear banner command was introduced.
3.1(1)	This command was changed to clear configure banner .

Examples The following example shows how to clear banners:

```
hostname(config)# clear configure banner
```

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 certificate 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:

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

Command History

Release	Modification
3.1(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 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:

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

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from clear class .

Examples The following example clears the class configuration:

```
hostname(config)# clear configure class
```

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** { **regex** | **inspect** [*protocol*] }]

Syntax Description	inspect	(Optional) Clears inspection class maps.
	<i>protocol</i>	(Optional) Specifies the type of application map you want to clear. Available types include: • http • 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.
	4.0(1)	The type keyword was added.

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 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:

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

Release	Modification
3.1(1)	This command was introduced.

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 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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Examples The following example shows how to reset the console connection settings to defaults:

```
hostname(config)# clear configure console
```

Command	Description
console timeout	Sets the idle timeout for a console connection to the FWSM.
show running-config console timeout	Displays the idle timeout for a console connection to the FWSM.

Related Commands

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from clear context .

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 trustpoints, all certificates, certificate map configurations, and ISAKMP, use the **clear configure crypto** command in global configuration mode. 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** | **isakmp** | **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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example issued in global configuration mode, removes all of the crypto configuration from the FWSM:

```
hostname(config)# clear configure crypto
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto	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 mode.

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:

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

Command History	Release	Modification
	3.1(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 mode.

clear configure crypto dynamic-map *dynamic-map-name* *dynamic-seq-num*

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of a specific crypto dynamic map.
<i>dynamic-seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear crypto dynamic-map .

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 map

To remove all or specified crypto maps from the configuration, use the **clear configure crypto map** command in global configuration mode.

clear configure crypto map *map-name seq-num*

Syntax Description

<i>map-name</i>	Specifies the name of a specific crypto map.
<i>seq-num</i>	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:

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

Command History

Release	Modification
3.1(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 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:

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

Release	Modification
3.1(1)	This command was introduced.

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
```

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Usage Guidelines The **clear 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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Examples The following example clears all DNS commands:

```
hostname(config)# clear configure dns
```

Related Commands	Command	Description
	dns domain-lookup	Enables the FWSM 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 FWSM 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 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from clear established .

Usage Guidelines To remove an established connection created by the **established** command, enter the **clear local-hosts** 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 local-hosts	Clears the current connections.

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:

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

Release	Modification
1.1(1)	This command was introduced (as clear failover).
3.1(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear filter .

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# 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 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:

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

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	In multiple context mode, you can enter this command within a context only. Previously, you entered it in the system execution space. This command was also changed from clear firewall .

Examples The following example sets the firewall mode to the default:

```
hostname(config)# clear configure firewall
```

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:

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

Command History

Release	Modification
1.1(1)	The clear fixup command was introduced.
3.1(1)	This command was changed from clear fixup .

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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	The clear fragment command was introduced.
3.1(1)	The configure keyword and optional <i>interface</i> 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.
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:

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

Command History

Release	Modification
3.1(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 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 ftp-map

To clear the FTP map configuration, use the **clear configure ftp-map** command in global configuration mode.

clear configure ftp-map

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
3.1(1)	This command was introduced.

Usage Guidelines

The **clear configure ftp-map** command removes the FTP map configuration.

Examples

The following example clears the FTP map configuration:

```
hostname# clear configure ftp-map
```

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.
request-command deny	Specifies FTP commands to disallow.

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:

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

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear global .

Examples The following example shows how to remove the **global** commands from the configuration:

```
hostname(config)# clear configure global
```

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-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

<i>name</i>	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:

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

Command History

Release	Modification
3.1(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 gtp-map

To clear GTP map configuration, use the **clear configure gtp-map** command in global configuration mode.

clear configure gtp-map

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
3.1(1)	This command was introduced.

Usage Guidelines

The **clear configure gtp -map** command removes the GTP map configuration.

Examples

The following example clears GTP map configuration:

```
hostname# clear configure gtp-map
```

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.

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 hostname is FWSM.

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	•	•	•	•	—

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The configure keyword was added.

Examples The following example clears the hostname:

```
hostname(config)# clear configure hostname
```

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 FWSM.

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 FWSM 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 FWSM.
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 http-map

To clear HTTP map configuration, use the **clear configure http-map** command in global configuration mode.

clear configure http-map

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
3.1(1)	This command was introduced.

Usage Guidelines

The **clear configure http-map** command removes the HTTP map configuration.

Examples

The following example clears the HTTP map configuration:

```
hostname# clear configure http-map
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
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.

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:

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

Command History

Release	Modification
3.1(1)	Support for 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 interface

To clear the interface configuration, use the **clear configure interface** command in global configuration mode.

clear configure interface[*mapped_name* | *interface_name*]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.

Defaults

If you do not specify an interface, the FWSM clears all interface configuration.

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
3.1(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 example clears the interface configuration:

```
hostname(config)# clear configure interface
```

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 interface bvi

To clear the bridge virtual interface configuration, use the **clear configure interface bvi** command in global configuration mode.

clear configure interface bvi *bridge_group_number*

Syntax Description

bridge_group_number Specifies the bridge group number as an integer between 1 and 100.

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
3.1(1)	This command was introduced.

Examples

The following example clears the interface configuration for bridge group 1:

```
hostname(config)# clear configure interface bvi 1
```

Related Commands

Command	Description
bridge-group	Groups two transparent firewall interfaces into a bridge group.
interface	Configures an interface.
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
ip address	Sets the management IP address for a bridge group.
show running-config interface bvi	Shows the bridge group interface configuration.

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:

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

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines In transparent firewall mode, this command clears the management IP address for the bridge groups. If you want to stop all current connections that use the old IP addresses, enter the **clear local-hosts** 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 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	<i>poolname</i> (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:

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Examples	The following example removes all IP address pools from the running configuration: <pre>hostname(config)# clear config ip local pool hostname(config)#</pre>

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:

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

Release	Modification
1.1(1)	The clear ip verify reverse-path command was introduced.
3.1(1)	This command was changed to clear configure 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

route	(Optional) Clears the commands that statically define routes in the IPv6 routing table from the running configuration.
access-list	(Optional) Clears the IPv6 access list commands 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:

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

Command History

Release	Modification
3.1(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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Examples The following example issued in global configuration mode, removes all of the ISAKMP configuration from the FWSM:

```
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 FWSM.
	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM.
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 logging

To clear the 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 reenabled. 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

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
3.1(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.

Examples

The following example shows how to clear logging configuration. 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 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
Global configuration	•	•	•	•	—

Release	Modification
3.1(1)	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:

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

Command History	Release	Modification
	3.1(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:

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

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from clear mac-learn .

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 <i>id</i> value.

clear configure management-access

To remove the configuration of an internal interface for management access of the FWSM, 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:

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

Release	Modification
3.1(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 FWSM:

```
hostname(config)# clear configure management-access
```

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 mgcp-map

To clear the MGCP map configuration, use the **clear configure mgcp-map** command in global configuration mode.

clear configure mgcp-map

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
3.1(1)	This command was introduced.

Usage Guidelines

The **clear configure mgcp-map** clears the MGCP map configuration.

Examples

The following example clears clear the MGCP map configuration:

```
hostname# clear configure mgcp-map
```

Related Commands

Commands	Description
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.
show mgcp	Displays information about MGCP sessions established through the FWSM.

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:

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

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines By default, virtual interfaces are not monitored for failover. Using the **clear monitor-interface** command clears the **monitor-interface** commands from the running configuration. To view the **monitor-interface** commands in the running configuration, use the **show running-config monitor-interface** command.

Examples The following example clears the **monitor-interface** commands from the running configuration:

```
hostname(config)# clear configure monitor-interface
hostname(config)#
```

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:

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

Release	Modification
3.1(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)#
```

Command	Description
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays configured multicast routes.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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:

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

Command History	Release	Modification
	3.1(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 FWSM.

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:

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

Command History

Release	Modification
1.1(1)	The clear name command was introduced.
3.1(1)	This command was changed to clear configure name .

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 privileged EXEC 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.1(1)	This command was changed from clear nat .

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

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 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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear object-group .

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:

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

Command History

Release	Modification
1.1(1)	The clear passwd command was introduced.
3.1(1)	This command was changed to clear configure 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 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 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
Global configuration	•	—	•	—	—

Release	Modification
3.1(1)	This command was introduced.

Command History

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
```

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.

Related Commands

clear configure policy-map

To remove 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.
<i>protocol</i>	(Optional) Specifies the type of inspection policy map you want to clear. Available types include: • dcerpc • esmtplib • http • sip

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
3.1(1)	This command was introduced.
4.0(1)	The type keyword was added.

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 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

<i>prefix-list-name</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as clear prefix-list).
3.1(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 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:

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

Release	Modification
1.1(1)	The clear privilege command was introduced.
3.1(1)	This command was changed from clear privilege .

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
```

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 prompt

To clear the customized prompt, use the **clear configure prompt** command in global configuration mode.

clear configure prompt

Syntax Description

This command has no arguments or keywords.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example clears the customized prompt:

```
hostname(config)# clear configure prompt
```

Related Commands

Command	Description
prompt	Creates a customized prompt.
show running-config prompt	Displays the configured prompt.

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:

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

Command History	Release	Modification
	4.0(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 resource partition

To clear the memory partition configuration, use the **clear configure resource partition** command in global configuration mode.

clear configure resource partition *[number]*

Syntax Description

number (Optional) Specifies the partition number, between 0 and 11 by default. If you changed the number of partitions using the **resource acl-partition** command, the partition numbering starts with 0. So if you have 10 partitions, the partition numbers are 0 through 9.

Defaults

Clears the configuration for all partitions if you do not specify a number.

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
4.0(1)	This command was introduced.

Examples

The following example clears the configuration for partition 0:

```
hostname(config)# clear configure resource partition 0
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.
resource rule	Reallocates rules between features globally for all partitions.
rules	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource partition	Shows the memory partition sizes.
show resource rule	Shows the current allocation of rules.

Command	Description
show running-config resource partition	Shows the current memory partition configuration.
size	Changes the size of a memory partition.

clear configure rip

To clear the **rip** commands from the running configuration, use the **clear configure rip** command in global configuration mode.

clear configure rip

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
Global configuration	•	—	•	—	—

Release	Modification
1.1(1)	This command was introduced (as clear rip).
3.1(1)	This command was changed from clear rip to clear configure rip .

Usage Guidelines The **clear configure rip** command removes all **rip** commands from the configuration. Use the **no** form of the commands to clear specific commands.

Examples The following example clears all RIP commands from the running configuration:

```
hostname(config)# clear configure rip
```

Command	Description
debug rip	Displays debug information for RIP.
rip	Configures RIP on the specified interface.
show running-config rip	Displays the RIP commands in the running configuration.

clear configure route-inject

To remove all the route-inject configurations, use the **clear configure route-inject** command in global configuration mode. The associated connected and static routes and NAT pools that were injected into the MSFC routing tables are also removed. You can remove the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if you are in single routed mode.

clear configure route-inject

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
Global configuration	•	—	•	• —	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **clear configure route-inject** command in global configuration mode remove all the route-inject configurations. The associated connected and static routes and NAT pools that were injected into the MSFC routing tables are also removed.

The **route-inject** command is used to inject the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.

Examples

The following example shows how to remove the conditions for the route injection:

```
hostname(config)# clear configure route-inject
```

Related Commands

Command	Description
debug route-inject	Enables debugging of the route-injections that have been configured on FWSM.
route-inject	Injects the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.

Command	Description
show route-inject	Displays the routes and NAT pools that have been injected.
show running-config route-inject	Displays the route-injection running configuration.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as clear route-map).
3.1(1)	This command was changed from clear route-map to clear configure route-map .

Usage Guidelines

Use the **clear configure route-map** command in global configuration mode to remove all **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 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 the information about the route map configuration.

clear configure router

To clear all router commands from the running configuration, use the **clear configure router** command in global configuration mode.

clear configure router [**ospf** [*id*] | **bgp** [*as-num*]]

Syntax Description

<i>as-num</i>	(Optional) The BGP autonomous system number.
bgp <i>as-num</i>	(Optional) Specifies that only BGP commands are removed from the configuration.
<i>id</i>	(Optional) The OSPF process ID.
ospf	(Optional) Specifies that only OSPF commands are removed from the configuration.

Defaults

If no keywords are specified, all **router** commands and associated sub-commands are cleared from the configuration.

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
1.1(1)	This command was introduced (as clear router).
3.1(1)	This command was changed from clear router to clear configure router .
3.2(1)	The bgp keyword was added.

Examples

The following example clears all OSPF commands associated with OSPF process 1 from the running configuration:

```
hostname(config)# clear configure router ospf 1
hostname(config)#
```

The following example clears all BGP commands associated with the BGP routing process with the autonomous system number of 100:

```
hostname(config)# clear configure router bgp 100
hostname(config)#
```

Related Commands

Command	Description
show running-config router	Displays the commands in the global router configuration.

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:

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

Release	Modification
3.1(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 snmp-map

To clear the SNMP map configuration, use the **clear configure snmp-map** command in global configuration mode.

clear configure snmp-map

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
3.1(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 Simple Network Management Protocol (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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Release	Modification
3.1(1)	Support for this command was introduced.

Examples This example shows how to disable the SNMP server:

```
hostname #clear 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:

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

Command History	Release	Modification
	3.1(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 FWSM from the specified client or network.
	ssh scopy enable	Enables a secure copy server on the FWSM.
	ssh timeout	Sets the timeout value for idle SSH sessions.
	ssh version	Restricts the FWSM to using either SSH Version 1 or SSH Version 2.

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:

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

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.1(1)	This command was changed from clear static .

Examples This example shows how to remove all the **static** commands from the configuration:

```
hostname(config)# clear configure static
```

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 FWSM, 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 FWSM.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **sunrpc-server** command displays the configured **router ospf** commands.



Note

If the highest-level IP address on the FWSM 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 FWSM:

```
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:

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

Release	Modification
1.1(1)	This command was introduced.
3.1(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 access lists 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 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:

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

Release	Modification
3.1(1)	The keyword configure was added.

Command History

Examples This example shows how to remove the Telnet connection and the idle timeout from the FWSM configuration:

```
hostname(config)# clear configure telnet
```

Command	Description
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the FWSM.
telnet	Adds Telnet access to the console and sets the idle timeout.

Related Commands

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:

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

Release	Modification
2.2(1)	The clear terminal command was introduced.
3.1(1)	This command was changed to clear configure terminal .

Examples The following example clears the display width:

```
hostname# clear configure terminal
```

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 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from clear timeout .

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 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:

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

Command History

Release	Modification
3.1(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 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear url-block .

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear url-cache .

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 filter command.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from clear url-server .

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. To clear the configuration for a particular user, use this command and append the username.

clear configure username [*name*]

Syntax Description

name (Optional) Specifies the username 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	The clear username command was introduced.
3.1(1)	This command was changed from clear username .

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 FWSM 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:

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

Command History	Release	Modification
	1.1(1)	The clear virtual command was introduced.
	3.1(1)	This command was changed from clear virtual .

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 FWSM and with the HTTP server.
	virtual telnet	Authenticates users with the virtual Telnet server for traffic types for which the FWSM does not supply an authentication prompt.

clear configure xlate-bypass

To set the xlate bypass configuration to the default (disabled), use the **clear configure xlate-bypass** command in global configuration mode.

clear configure xlate-bypass

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	•	•	•	•	—

Release	Modification
3.2(1)	This command was introduced.

Command History

Examples The following example clears the xlate bypass configuration:

```
hostname(config)# clear configure xlate-bypass
```

Command	Description
nat	Configures NAT.
nat-control	Enables NAT control.
same-security-traffic inter-interface	Allows interfaces on the same security level to communicate.
show xlate	Shows current translation and connection information.
xlate-bypass	Enables xlate bypass.

Related Commands



CHAPTER

7

clear console-output through clear xlate Commands

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:

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines The FWSM automatically captures output destined for the internal console port. Do not use the internal console port unless you are advised to do so by Cisco TAC.

Examples The following example shows how to remove the currently captured console output:

```
hostname# clear console-output
```

Command	Description
show console-output	Displays the captured console output.

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	(Multiple mode only) Clears counters for all contexts.
context <i>context-name</i>	(Multiple mode only) Clears counters for the specified context name.
:counter_name	(Optional) Clears the specified counter.
detail	(Optional) Clears detailed counter information.
protocol <i>protocol_name</i>	(Optional) Clears the counters for the specified protocol.
summary	(Multiple mode only) Clears counters for all contexts.
threshold <i>n</i>	(Optional) Clears the counters at or above the specified threshold. The range is 1 through 4294967295.
top <i>n</i>	(Multiple mode only) Clears a counter for the contexts that are the top <i>n</i> users of the counter. You must specify a counter name with this option. The range is 1 through 4294967295.

Defaults

By default, the FWSM clears all counters.

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
2.2(1)	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.
show counters description	Shows a list of protocol counters.

clear crashinfo

To delete the contents of the crash file in Flash memory, enter 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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Usage Guidelines This command has no usage guidelines.

Examples The following example shows how to delete the crash file:

```
hostname# clear crashinfo
```

crashinfo force	Forces a crash of the FWSM.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the FWSM to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file stored in Flash memory.

Related Commands

clear crypto accelerator statistics

To clear the global and accelerator-specific statistics from the crypto accelerator MIB, use the **clear crypto accelerator statistics** command in privileged EXEC modes.

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:

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

Command History	Release	Modification
	3.1(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 global configuration 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:

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

Command History

Release	Modification
3.1(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 FWSM:

```
hostname(config)# clear crypto ca crls
hostname(config)#
```

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 protocol statistics

To clear the protocol-specific statistics in the crypto accelerator MIB, use the **clear crypto protocol statistics** command in privileged EXEC modes.

clear crypto protocol statistics *protocol*

Syntax Description

<i>protocol</i>	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 Sockets 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, clears all crypto accelerator statistics:

```
hostname(config)# clear crypto protocol statistics all
hostname(config)#
```

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 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:

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

Release	Modification
2.2(1)	This command was introduced.

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:

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

Release	Modification
3.1(1)	This command was introduced.

Examples The following example clears the DNS cache:

```
hostname# clear dns-hosts cache
```

Command	Description
dns domain-lookup	Enables the FWSM 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 FWSM 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	<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are clearing the event log. Because the FWSM 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:

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

Command History	Release	Modification
	4.0(1)	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

<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
<i>if-name</i>	(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.
<i>ip-addr</i>	(Optional) The IP address of the neighbor you want to remove from the neighbor table.
soft	Causes the FWSM 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:

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

Command History

Release	Modification
4.0(1)	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

<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
<i>ip-addr</i>	The IP address to clear from the topology table.
<i>mask</i>	(Optional) The network mask to apply to the <i>ip-addr</i> argument.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
4.0(1)	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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

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#
```

Command	Description
debug fover	Displays failover debug information.
show failover	Displays information about the failover configuration and operational statistics.

Related Commands

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	<i>interface</i>	(Optional) Specifies the FWSM interface.
	queue	Clears the IP fragment reassembly queue.
	statistics	Clears the IP fragment reassembly statistics.

Defaults	If an <i>interface</i> is not specified, the command applies to all interfaces.

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
	1.1(1)	This command was introduced.
	3.1(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: <pre>hostname# clear fragment queue</pre>

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.

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 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:

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

Release	Modification
1.1(1)	This command was introduced.

Examples The following example shows how to remove the garbage collection process statistics:

```
hostname# clear gc
```

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

<i>if_name</i>	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.

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
3.1(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

<i>group</i>	IGMP group address. Specifying a particular group removes the specified group from the cache.
<i>interface name</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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
```

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:

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

Command History	Release	Modification
	3.1(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 [mapped_name | interface_name]
```

Syntax Description	<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
	<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.

Defaults By default, this command clears all interface statistics.

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
	1.1(1)	This command was introduced.

Usage Guidelines

The **clear interface** command clears all interface statistics except the number of input bytes. See the **show interface** command for detail about interface statistics.

If an interface is shared among contexts, and you enter this command within a context, the FWSM clears only statistics for the current context. If you enter this command in the system execution space, the FWSM 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 bgp

To reset BGP connections to the neighbor and reset connection counters, use the **clear ip bgp** command in privileged EXEC mode.

clear ip bgp *neighbor-addr*

Syntax Description	<i>neighbor-addr</i>	The IP address of the BGP peer.

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 ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History	Release	Modification
	3.2(1)	This command was introduced.

Usage Guidelines	In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples	The following example resets the connection to the BGP neighbor with the address 10.1.1.1 and clears the associated statistical counters: <pre>hostname# clear ip bgp 10.1.1.1</pre>

Related Commands	Command	Description
	clear configure router	Clears the router commands from the running configuration.
	show ip bgp summary	Displays general information about the BGP routing process.

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 Sets the interface on which you want to clear Unicast RPF statistics.
interface_name

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
3.1(1)	This command was introduced.

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 <i>map-name</i>	(Optional) Clears IPsec SAs for the specified crypto map.
peer	(Optional) Clears IPsec SAs for a specified peer.
<i>peer-addr</i>	Specifies the IP address of an IPsec peer.
<i>protocol</i>	Specifies an IPsec protocol: esp or ah .
<i>spi</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example 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:

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

Command History

Release	Modification
3.1(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 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:

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

Release	Modification
3.1(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#

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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines 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
  unreachable: 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
```

■ clear ipv6 traffic

```

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 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples The following example removes the IKE runtime SA database from the configuration:

```
hostname(config)# clear isakmp sa
hostname(config)#
```

Related Commands	Command	Description
	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 FWSM.
	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 remove network connections, use the **clear local-host** command in privileged EXEC mode.

```
clear local-host [ip_address] [all]
```

Syntax Description	all	(Optional) Clears all connections, except for those directly to the FWSM and from the FWSM.
	<i>ip_address</i>	(Optional) Specifies the host IP address for which you want to clear connections.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History	Release	Modification
	1.1(1)	This command was introduced.

Examples

The following example clears all connections from 10.1.1.15:

```
hostname# clear local-host 10.1.1.15
```

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:

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

Release	Modification
3.1(1)	This command was changed from the show pdm logging command to the show asdm log command.

Usage Guidelines ASDM syslog messages are stored in a separate buffer from the FWSM syslog messages. Clearing the ASDM logging buffer only clears the ASDM syslog messages, it does not clear the FWSM system 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)#
```

Command	Description
show asdm log sessions	Displays the contents of the ASDM logging buffer.

clear logging buffer

To clear the logging buffer, use the **clear logging buffer** command in global configuration mode.

clear logging buffer

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Release	Modification
3.1(1)	This command was introduced.

Command History

Examples The following example shows how to remove all syslog messages from the internal log buffer:

```
hostname #clear logging buffer
```

Command	Description
logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
show logging	Displays the enabled logging options.

Related Commands

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	<i>interface_name</i> (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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.

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:

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

Release	Modification
3.1(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 configuration 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:

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

Command History

Release	Modification
3.1(1)	Support for 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 FWSM.

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

<i>group</i>	(Optional) IP address of the multicast group.
<i>source</i>	(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example clears all MFIB route counters:

```
hostname# clear mfib route counters
```

Related Commands

Command	Description
show mfib count	Displays MFIB route and packet count data.

clear ospf

To clear OSPF process information, use the **clear ospf** command in privileged EXEC mode.

```
clear ospf [pid] {process | counters [neighbor [neighbor-intf] [neighbor-id]]}
```

Syntax Description	counters	Clears the OSPF counters.
	neighbor	Clears the OSPF neighbor counters.
	<i>neighbor-intf</i>	(Optional) Clears the OSPF interface router designation.
	<i>neighbor-id</i>	(Optional) Clears the OSPF neighbor router ID.
	<i>pid</i>	(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.

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
	3.1(1)	This command was introduced.

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.

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 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	•	—	•	—	—

Release	Modification
3.1(1)	This command was introduced.

Command History

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
```

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.

Related Commands

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

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
```

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.

Related Commands

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:

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

Command History

Release	Modification
3.1(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 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**] [**resource** {*resource_name* | **all**}]

Syntax Description

context <i>context_name</i>	(Multiple mode only) Specifies the context name for which you want to clear statistics. Specify all for all contexts.
resource <i>resource_name</i>	Clears the usage of a specific resource. Specify all (the default) for all resources. Resources include the following types: • conns—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • hosts—Hosts that can connect through the FWSM. • ipsec—(Single mode only) IPSec sessions • ssh—SSH sessions. • telnet—Telnet sessions. • xlates—NAT translations.
summary	(Multiple mode only) Clears the combined context 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
2.2(1)	This command was introduced.

Examples

The following example clears all resource usage statistics:

```
hostname# clear resource usage
```

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 FWSM.

clear route

To remove dynamically learned routes from the routing table, use the **clear route** command in privileged EXEC mode.

clear route [statistics]

Syntax Description

statistics (Optional) Clears route statistical counters.

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
1.1(1)	This command was introduced.

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 statistics 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 <i>intf</i>	(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:

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

Command History

Release	Modification
3.1(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.
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.
<i>ap_name</i>	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.
<i>IMSI_value</i>	Hexadecimal value that identifies the specific IMSI.
interface	(Optional) Identifies a specific interface.
<i>int</i>	Identifies the interface for which information will be cleared.
<i>IP_address</i>	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.
<i>tunnel_ID</i>	Hexadecimal value that identifies the specific tunnel.
version	(Optional) Clears the PDP contexts based on the GTP version.
<i>version_num</i>	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:

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

Command History

Release	Modification
3.1(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 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:

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

Command History

Release	Modification
1.1(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 sunrpc-server active

To clear the pinholes opened by Sun RPC application inspection, use the **clear sunrpc-server active** command in global configuration 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:

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

Command History

Release	Modification
2.2(1)	Support for this command was introduced.
3.1(1)	This command was changed from clear rpc-server .

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 FWSM.

Examples

The following example shows how to clear the SunRPC services table:

```
hostname(config)# clear sunrpc-server
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the FWSM.
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.
sunrpc-server	Creates entries in the SunRPC services table.

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:

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

Release	Modification
1.1(1)	This command was introduced.

Command History

Usage Guidelines The **clear traffic** command resets the counters for transmit and receive activity that is displayed with the **show traffic** command.

Examples The following example shows the **clear traffic** command:

```
hostname# clear traffic
```

Command	Description
show traffic	Displays the counters for transmit and receive activity.

Related Commands

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	<i>username</i> (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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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 FWSM 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 rlee to reauthenticate:

```
hostname(config)# clear uauth rlee
```

Related Commands

Command	Description
aaa authentication	Enable or disable user authentication.
aaa authorization	Enable or disable user authorization.
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:

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

Release	Modification
1.1(1)	The clear url-block command was introduced.
3.1(1)	This command was changed from clear url-block .

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
	1.1(1)	The clear url-cache command was introduced.
	3.1(1)	This command was changed from clear url-cache .

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 that 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:

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

Release	Modification
1.1(1)	The clear url-server command was introduced.
3.1(1)	This command was changed from clear url-server .

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 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 <i>ip1[-ip2]</i>	(Optional) Clears the active translations by global IP address or range of addresses.
gport <i>port1[-port2]</i>	(Optional) Clears the active translations by the global port or range of ports.
interface <i>if_name</i>	(Optional) Displays the active translations by interface.
local <i>ip1[-ip2]</i>	(Optional) Clears the active translations by local IP address or range of addresses.
lport <i>port1[-port2]</i>	(Optional) Clears the active translations by local port or range of ports.
netmask <i>mask</i>	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state <i>state</i>	(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 norandomseq 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

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. Static xlates can only be removed by removing the **static** command from the configuration; the **clear xlate** 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** 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** 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** 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 FWSM, 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.
<i>priority</i>	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 FWSM ignores it.
type <i>type</i>	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 <i>version</i>	Identifies the device version via free-form strings. 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Construct rules according to these caveats:

- If you do not define any rules, the FWSM permits all connection types.
- When a client matches none of the rules, the FWSM denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the FWSM 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-firewall

To set personal firewall policies that the FWSM 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.

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-zonealarm 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 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-security-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 FWSM checks to make sure the firewall is running. It asks, "Are You There?" If there is no response, the FWSM 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-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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Only one instance of this command can be configured.

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.

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-update

To configure and change client update parameters, 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. You can specify up to 4 of these client update entries.

To disable a client update, use the **no** form of this command.

client-update *type* {**url** *url-string*} {**rev-nums** *rev-nums*}

no client-update [*type*]

Syntax Description

rev-nums <i>rev-nums</i>	Specifies the software or firmware images for this client. Enter up to 4, separated by commas.
<i>type</i>	Specifies the operating systems to notify of a client update. The list of operating systems comprises the following: - 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
url <i>url-string</i>	Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client.

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
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only. 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.

Examples

The following example entered in config-ipsec configuration mode, configures client update parameters for the remote-access tunnel-group remotegrp. It designates the revision number, 4.6.1 and the URL for retrieving the update, which is <https://support/updates>.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# client-update type windows url https://support/updates/ rev-nums
4.6.1
hostname(config-ipsec)#
```

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-map enable	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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

<i>mode</i>	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 .
<i>command_alias</i>	Specifies the new name you want for an existing command.
<i>original_command</i>	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:

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

Command History

Release	Modification
3.1(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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MGCP map configuration	•	•	•	•	No

Command History

Release	Modification
3.1	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.
show mgcp	Displays MGCP configuration and session information.

Commands	Description
timeout [mgcp]	Configures the idle timeout after which an MGCP media connection will be closed.
timeout [mgcp-pat]	Configures the idle timeout after which an MGCP PAT xlate will be removed.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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.
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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.

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 FWSM, 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

<i>:filename</i>	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 FWSM 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 (:).
<i>server:</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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
```

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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

<i>url</i>	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax: • disk:<i>/[path/]filename</i> This URL indicates the internal Flash memory. • ftp:<i>//[user[:password]@]server[:port]/[path/]filename[;type=xx]</i> The FTP path on the server is a relative path (<i>path/filename</i>). To use an absolute path (<i>/path/filename</i>), enter an extra slash (/) after the server address: ftp://server/[path/]filename 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]:<i>//[user[:password]@]server[:port]/[path/]filename</i> • tftp:<i>//[user[:password]@]server[:port]/[path/]filename[;int=interface_name]</i> 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:

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

Command History

Release	Modification
2.2(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 FWSM 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 FWSM 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 FWSM 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 vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# class gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# class silver
```

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 FWSM, 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **console timeout** command does not alter the Telnet or SSH timeouts; these access methods maintain their own timeout values using the **timeout** command.

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.
show running-config console timeout	Displays the idle timeout for a console connection to the FWSM.
timeout	Sets the idle time for connection, translation UDP, and RPC slots.

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, which is accessible using the **http-map** command. 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:

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

After enabling the **content-length** command, the FWSM only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the FWSM 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 FWSM 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.

content-type-verification

To restrict HTTP traffic based on the content type of the HTTP message, use the **content-type-verification** command, in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a message fails command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generates a syslog message.
match-req-rsp	(Optional) Verifies that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message.
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:

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

Command History

Release	Modification
3.1	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.
- The **match-req-rsp** keyword enables an additional check that 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 FWSM 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 restricts HTTP traffic based on the content type of the HTTP message. If a message contains an unsupported content type, the FWSM resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp 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

<i>name</i>	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:

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

Command History

Release	Modification
2.2(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 vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

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.

control-point tcp-normalizer

To enable the TCP normalizing function, use the **control-point tcp-normalizer** command in global configuration mode. The TCP normalizer performs the following action: for traffic that passes through the control-plane path, such as packets that require Layer 7 inspection or management traffic, the FWSM sets the maximum number of out-of-order packets that can be queued for a TCP connection to 2 packets. The TCP normalizer is enabled by default, and is not configurable except to enable or disable it. To disable the TCP normalizer, use the **no** form of the command.

```
control-point tcp-normalizer

no control-point tcp-normalizer
```

Syntax Description This command has no arguments or keywords.

Defaults The TCP normalizer 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
Global configuration	•	•	•	•	—

Release	Modification
3.1(4)	This command was introduced.

Usage Guidelines You might want to disable the TCP normalizer for testing purposes.

When you disable the TCP normalizer, new flows do not use the TCP normalizer, but existing flows continue to use the TCP normalizer.

Examples The following example disables the TCP normalizer:

```
hostname(config)# no control-point tcp-normalizer
```

Command	Description
set connection	Sets connection limits.

copy

To copy a file from one location to another, use the **copy** command.

copy [/noconfirm] {url | running-config | startup-config} {running-config | startup-config | url}

Syntax Description		
	/noconfirm	Copies the file without a confirmation prompt.
	running-config	Specifies the running configuration.
	startup-config	Specifies the startup configuration. 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 FWSM 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:

- **disk:***/[path/]filename*

This option indicates the configuration partition of the internal flash memory.

- **ftp:***//[user[:password]@]server[:port]/[path/]filename[;type=xx]*

The FTP path on the server is a relative path (*path/filename*). To use an absolute path (*/path/filename*), enter an extra slash (*/*) after the server address:

ftp:*//server/[path/]filename*

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.

The path after the server address is a relative path (*path/file*). To make it an absolute path (*/path/file*), use two slashes after the server, for example:

tftp:*//server/[path/]filename*

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
Privileged mode	•	•	•	•	•

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	The ability to copy from a context to a server was added.

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

This example shows how to copy a file from the disk to a TFTP server in the system execution space:

```
hostname(config)# copy disk:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

**Note**

If the **tftp-server** command defines an interface different than the location you wish to copy the a file from, you must use the **int** keyword to override the interface specified in the **tftp-server** command, or the device will attempt to copy the file from that interface.

This 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 disk:my_context.cfg disk:my_context/my_context.cfg
```

This example shows how to copy an ASDM file from a TFTP server to the flash partition:

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin flash:asdm
```

This 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
```

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.
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	Specifies a 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: disk:<i>/[path/]filename</i> This option indicates the configuration partition of the internal Flash memory. ftp:<i>//[user[:password]@]server[:port]/[path/]filename[;type=xx]</i> The FTP path on the server is a relative path (<i>path/filename</i>). To use an absolute path (<i>/path/filename</i>), enter an extra slash (<i>/</i>) after the server address: ftp://server//[path/]filename 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]:<i>//[user[:password]@]server[:port]/[path/]filename</i> tftp:<i>//[user[:password]@]server[:port]/[path/]filename[;int=interface_name]</i> 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	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

In multiple context mode, enter this command in the system execution space; you cannot enter this command within a context.

Examples

This example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
hostname# 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# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

If the TFTP server is already configured, the location or filename can be overridden as follows:

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

In multiple context mode, to copy a capture from within a context, you must specify the context name:

```
hostname/Context1# capture abc access-list test interface inside
hostname/Context1# changeto system
hostname# copy capture:Context1/abc tftp:171.68.11.129/tftpboot/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.

copy optimized-running-config

To replace the original non-optimized access lists with the optimized access lists, use the **copy optimized-running-config** command in privileged EXEC mode.

copy optimized-running-config running-config

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 mode	•	•	•	•	•

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Having access list optimization enabled at all times could be a waste of computational and memory resources. If you are satisfied with how the optimized access lists are merged, you can replace the original access lists with the optimized ones. Note that this action will wipe out all of the original access lists. After copying the optimized access lists, you may want to disable access list optimization because the newly copied optimized access lists may not be further optimized.

Examples The following example shows how to replace the original non-optimized access lists with the optimized ones:

```
hostname(config)# copy optimized-running-config running-config
```

Command	Description
access-list optimization enable	Enables access list optimization.
show running-config access-list	Displays the current running access-list configuration.
debug acl optimization	Debugs access list optimization.
write memory	Saves the running configuration to the startup configuration.

cpu threshold rising

To enable configuration of the CPU threshold, use the **cpu threshold rising** command in global configuration mode. To disable configuration, use the **no** form of this command.

[no] cpu threshold rising [*threshold_value%*] [*monitoring_interval*]

Syntax Description

monitoring_period	Sets the CPU usage monitoring period (60-3600 sec).
threshold_value	Sets the CPU usage threshold value (10-100%).

Defaults

The default configuration has the CPU threshold and monitoring period disabled.

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
3.2(1)	This command was introduced.

Usage Guidelines

To send CPU threshold information to the NMS, enter the **logging history** command, and enable logging using the **logging enable** command. To remove the cpu threshold configuration, use the **clear config all** or **clear config cpu** command.



Note

In system mode, if the CPU threshold and monitoring interval are configured, these values are effective only when the **snmp-server enable traps cpu threshold** command is configured in Admin context.

Examples

The following example configures the CPU utilization threshold value as 75% and the monitoring period as 300 seconds.

■ **cpu threshold rising**

```

hostname(config)# cpu?
configure mode commands/options:
threshold Configure CPU utilization threshold parameters
exec mode commands/options:
profile CPU profiler
hostname (config)# cpu threshold?
configure mode commands/options:
rising Configure CPU rising threshold parameters
hostname (config)# cpu threshold rising?
configure mode commands/options:
WORD CPU rising threshold value (10-100%)
hostname (config)# cpu threshold rising 75?
configure mode commands/options:
60-3600 CPU rising threshold monitoring period (60-3600 seconds)
hostname (config)# cpu threshold rising 75% 300

```

Related Commands

Command	Description
snmp-server enable	Enables SNMP on the FWSM.
snmp-server enable traps	Enables SNMP traps on the FWSM.

crashinfo force

To force the FWSM 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 FWSM as a result of a page fault.
watchdog	(Optional) Forces a crash of the FWSM as a result of watchdogging.

Defaults

The FWSM 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:

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

Command History

Release	Modification
3.1	This command was introduced.

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 FWSM 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 FWSM 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 FWSM crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a **no**, and the FWSM 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 FWSM 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.

crashinfo save disable

no crashinfo save disable

Syntax Description

This command has no default arguments or keywords.

Defaults

The FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM crashes during startup, the crash information file is not saved. The FWSM 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 FWSM.
crashinfo test	Tests the ability of the FWSM 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 FWSM to save crash information to a file in Flash memory, use the **crashinfo test** command in global configuration 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:

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

Release	Modification
3.1(1)	This command was introduced.

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 FWSM.

Examples The following example shows the output of a crash information file test.

```
hostname(config)# crashinfo test
```

clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces the FWSM 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 FWSM can still accept the peer certificate if the required CRL is not available.
nocheck	Directs the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 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:

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

Release	Modification
3.1(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 submode.



crypto ca authenticate through crypto map set trustpoint 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 FWSM uses to authenticate the CA certificate. If a fingerprint is provided, the FWSM 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 FWSM displays the computed fingerprint and asks whether to accept the certificate.
<i>hexvalue</i>	Identifies the 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 FWSM accepts the certificate without question.
<i>trustpoint</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If the trustpoint is configured for SCEP enrollment, the CA certificate is downloaded through SCEP. If not, the FWSM 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

In the following example, the FWSM requests the certificate of the CA. The CA sends its certificate and the FWSM prompts the administrator to verify the certificate of the CA by checking the CA certificate fingerprint. The FWSM administrator should verify the fingerprint value displayed against a known, correct value. If the fingerprint displayed by the FWSM 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 the FWSM prompts the administrator to paste the CA certificate to the terminal. After displaying the fingerprint of the certificate, the FWSM 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
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUEwETAPBgNVBACTECZyYW5rbGluMREw
DwYDVQQDEwhCcm1hbnNDQTAeFw0wMjEwMTcxODE5MTJhFw0wNjEwMTcxODE5MTJh
MEAxCAAJBgNVBAYTA1VTMQswCQYDVQQIEwJNTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUBCP5aWKfQViKJENzI2GnAheArazaAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYtvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE740vKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhZCCAYMwEwYJ
KwYBBAGCNxQCBAYeBADAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHR3holowFDmniI3FBWkpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnlIs
Q049Q0RQLENOPVB1YmXpYyUyMETleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMSREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOY2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbmQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VyDEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEW
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgAlr
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGgla3tevYVwhHNPA4mWo
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 **no** form of the command or use the **exit** command.

crypto ca certificate chain *trustpoint*

[no] 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:

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

Command History

Release	Modification
3.1(1)	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*

no crypto ca certificate map [*sequence-number*]

Syntax Description

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.

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
3.1(1)	This command was introduced.

Usage Guidelines

Issuing this command places the FWSM in CA certificate map configuration mode where you 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*. DN's 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 <i>tag</i>	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 sequence number of 1 (rule # 1) and specifies that the common name(CN) attribute of the subject-name must match Pat:

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr cn eq pat
hostname(ca-certificate-map)#
```

The following example enters CA certificate map mode with a sequence number of 1 and specifies that the subject-name contain the value cisco anywhere within it:

```
hostname(config)# crypto ca certificate 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:

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

Command History

Release	Modification
3.1(1)	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 configure 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.
<i>trustpoint</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When the trustpoint is configured for SCEP enrollment, the FWSM displays a CLI prompt immediately and displays status messages to the console asynchronously. When the trustpoint is configured for manual enrollment, the FWSM 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 FWSM 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:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIB3DQEU
AhYTd2ItMjYwMCOzLmNpc2NvLmNvbTBcMA0GCSqGSIB3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULWlKF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQM4GA1UdDwEB
/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 in PKCS12 format the keys and certificates associated with a trustpoint configuration, use the **crypto ca export** command in global configuration mode.

crypto ca export *trustpoint* **pkcs12** *passphrase*

Syntax Description

<i>passphrase</i>	Specifies the passphrase used to encrypt the PKCS12 file for export.
pkcs12	Specifies the public key cryptography standard to use in exporting the trustpoint configuration.
<i>trustpoint</i>	Specifies the name of the trustpoint whose certificate and keys are to be exported. When you export, if the trustpoint uses RSA keys, the exported key pair is assigned the same name as the trustpoint.

Defaults

This command has no default 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
3.1(1)	This command was introduced.

Usage Guidelines

Invocations of this command do not become part of the active configuration. The PKCS12 data is written to the terminal.

Examples

The following example exports PKCS12 data for trustpoint central using xxyyzz as the passcode:

```
hostname(config)# crypto ca export central pkcs12 xxyyzz
```

Exported pkcs12 follows:

```
[ PKCS12 data omitted ]
```

```
---End - This line not part of the pkcs12---
```

Related Commands	Command	Description
	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 authenticate	Obtains the CA certificate for this trustpoint.
	crypto ca enroll	Starts enrollment with a CA.
	crypto ca trustpoint	Enters the trustpoint submode 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 FWSM 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

<i>trustpoint</i>	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 FWSM to import a certificate from the CA represented by the trustpoint.
pkcs12	Tells the FWSM to import a certificate and key pair for a trustpoint, using PKCS12 format.
<i>passphrase</i>	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:

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

Command History

Release	Modification
3.1(1)	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
```

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
```

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 trustpoint

To add a trustpoint and enter trustpoint configuration mode, use the **crypto ca trustpoint** command in global configuration mode. To remove the specified trustpoint, use the **no** form of this command. 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 trustpoint commands control CA-specific configuration parameters which specify how the FWSM obtains the CA certificate, how the FWSM obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

Syntax Description	noconfirm	(Optional) Suppresses all interactive prompting
	<i>trustpoint- name</i>	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:

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Usage Guidelines A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. The trustpoint commands control CA-specific configuration parameters which specify how the FWSM obtains the CA certificate, how the FWSM obtains its certificate from the CA, and the authentication policies for user certificates issued by the CA.

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 crt 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 define a dynamic crypto map entry, use the **crypto dynamic-map match address** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. See the **crypto map match address** command for additional information about 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

<i>acl-name</i>	Identifies the access list to be matched for the dynamic crypto map entry.
<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

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 peer

To define a dynamic crypto map entry, use the **crypto dynamic-map set peer** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. 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

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
<i>ip_address</i>	Identifies the peer in the dynamic crypto map entry by IP address, as defined by the name command.
<i>hostname</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

Examples

The following example shows setting a peer for a dynamic-map named mymap to the IP address 10.0.0.1:

```
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 define a dynamic crypto map entry, use the **crypto dynamic-map set pfs** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. 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** | **group7**]

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group7**]

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	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.
group7	Specifies that IPsec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the MovianVPN client.
set pfs	Configures IPsec to ask for perfect forward secrecy 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

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 FWSM 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 FWSM 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

To define a dynamic crypto map entry, use the **crypto dynamic-map set reverse route** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. 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

<i>dynamic-map-name</i>	Specifies the name of the crypto map set.
<i>dynamic-seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

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 security-association lifetime

To define a dynamic crypto map entry, use the **crypto dynamic-map set security-association lifetime** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. See the **crypto map set security-association lifetime** command for additional information about this command.

crypto dynamic-map *dynamic-map-name dynamic-seq-num set security-association lifetime seconds seconds | kilobytes kilobytes*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num set security-association lifetime seconds seconds | kilobytes kilobytes*

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
<i>kilobytes</i>	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.
<i>seconds</i>	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

Examples

The following command specifies a security association lifetime in seconds for crypto dynamic-map mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set security-association lifetime seconds 1400
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 define a dynamic crypto map entry, use the **crypto dynamic-map set transform-set** command in global configuration mode. Use the **no** form of this command to remove the access list from a crypto map entry. See the **crypto map set transform-set** command for additional information about this command.

crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set transform-set** *transform-set-name1* [... *transform-set-name9*]

no crypto dynamic-map *dynamic-map-name* *dynamic-seq-num* **set transform-set** *transform-set-name1* [... *transform-set-name9*]

Syntax Description

<i>dynamic-map-name</i>	Specifies the name of the dynamic crypto map set.
<i>dynamic-seq-num</i>	Specifies the sequence number that corresponds to the dynamic crypto map entry.
<i>transform-set-name1</i> <i>transform-set-name9</i>	Identifies the transform set to be used with the dynamic crypto map entry (the names of transform sets defined using the crypto ipsec command).



Note

The **crypto map set transform-set** command is required for dynamic crypto map entries. All you need in the entry is a transform set.

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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from crypto dynamic-map .

Examples

The following command specifies two transform sets (tfset1 and tfset2) for the crypto dynamic-map mymap:

```
hostname(config)# crypto dynamic-map mymap 10 set transform-set tfset1 tfset2
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 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 FWSM may fragment the packet to add the IPSec encapsulation.
copy-df	(Optional) Specifies that the FWSM 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 FWSM may fragment the packet if the original packet had the DF bit cleared.
<i>interface</i>	Specifies an interface name.
token	Indicate a token-based server for user authentication is used.

Defaults

This command is disabled by default. If this command is enabled without a specified setting, the FWSM uses the **copy-df** setting as 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The DF bit with IPSec tunnels feature lets you specify whether the FWSM 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 FWSM 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, specifies 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 FWSM to fragment IPSec packets that are close to the maximum MTU size after encryption (disables pre-fragmentation).
before-encryption	Specifies the FWSM to fragment IPSec packets that are close to the maximum MTU size before encryption (enables pre-fragmentation).
<i>interface</i>	Specifies an interface name.
token	Indicate a token-based server for user authentication is used.

Defaults

This feature 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When a packet is near the size of the MTU of the outbound link of the encrypting FWSM, 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 decrypting device performance 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 on the interface:

```
hostname(config)# crypto ipsec fragmentation before-encryption mgmt  
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 mgmt  
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

<i>kilobytes</i>	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 kilobytes. The default is 4,608,000 kilobytes.
<i>seconds</i>	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	Indicate 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM 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 FWSM lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the FWSM 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 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, such as global lifetimes and transform sets.
show running-config crypto map	Displays all configuration for all the crypto maps.

crypto ipsec transform-set

To define a transform set, use the **crypto ipsec transform-set** command in global configuration mode. With this command, you identify the IPSec encryption and hash algorithms to be used by the transform set. Use the **no** form of this command to remove a transform set.

crypto ipsec *map-name seq-num* **transform-set** *transform-set-name transform1 [transform2]*

no crypto ipsec *map-name seq-num* **transform-set** *transform-set-name*

Syntax Description

esp-aes	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 128-bit key.
esp-aes-192	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 192-bit key.
esp-aes-256	Specifying this option means that IPSec messages protected by this transform are encrypted using AES with a 256-bit key.
esp-des	Specifying this option means that IPSec messages protected by this transform with encryption using 56-bit DES-CBC.
esp-3des	Specifying this option means that IPSec messages protected by this transform are encrypted using the Triple DES algorithm.
esp-none	Specifying this option means that IPSec messages do not use HMAC authentication.
esp-null	Specifying this option means that IPSec messages are not encrypted using the IPSec security protocol (ESP) only.
esp-md5-hmac	Specifying this option means that IPSec messages protected by this transform are using MD5/HMAC-128 as the hash algorithm.
esp-sha-hmac	Specifying this option means that IPSec messages protected by this transform are using SHA/HMAC-160 as the hash algorithm.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>transform1, transform2</i>	Specifies up to two transforms. Transforms define the IPSec security protocol(s) and algorithm(s). Each transform represents an IPSec security protocol (ESP), plus the algorithm to use, either [esp-aes esp-aes-192 esp-aes-256 esp-des esp-3des esp-null] or [esp-md5-hmac esp-sha-hmac] as defined in this syntax table.
<i>transform-set-name</i>	Specifies the name of the transform set to create or modify.
token	Indicate a token-based server for user authentication is used.

Defaults

The default encryption algorithm is esp-3des (Triple DES).

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
1.1(1)	This command was introduced.

Usage Guidelines

A transform set specifies one or two IPSec security protocols and specifies which algorithms to use with the selected security protocol. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPSec messages can be protected by a transform set using AES with a 128-bit key, 192-bit key, or 256-bit key.

Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman group 5 instead of group 1 or group 2. To do this, use the **isakmp policy priority group 5** command.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry in the IPSec security association negotiation protects the data flows specified by that crypto map entry's access list. During the negotiation, the peers search for a transform set that is the same at both peers. When the FWSM finds such a transform set, it applies it to the protected traffic as part of both peer's IPSec security associations.

Each transform-set represents an algorithm to use for encryption or authentication. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

Examples of acceptable transform combinations are as follows:

- **esp-des**
- **esp-des** and **esp-md5-hmac**

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms replace the existing transforms for that transform set.

Examples

The following example configures two transform sets: one named t1, using DES for encryption and SHA/HMAC-160 as the hash algorithm, and the other named standard, using AES 192 for encryption and MD5/HMAC-128 as the hash algorithm:

```
hostname(config)# crypto ipsec transform-set t1 esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set standard esp-aes-192 esp-md5-hmac
hostname(config)
```

Related Commands

Command	Description
clear configure crypto	Clears all IPSec configuration (that is, global lifetimes and transform sets).
show running-config crypto map	Displays all configuration for all the crypto maps.

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 <i>key-pair-label</i>	Specifies the name to be associated with the key pair(s); maximum label length is 128 characters. DSA requires a label.
modulus <i>size</i>	(Optional) Specifies the modulus size of the key pair(s): 512, 768, 1024. The default modulus size is 1024.
noconfirm	(Optional) 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
3.1(1)	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 FWSM displays an error message.

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	(Optional)	Generates a single pair of general purpose keys. This is the default key-pair type.
label <i>key-pair-label</i>	(Optional)	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 FWSM displays an warning message. If no label is provided when the key is generated, the key pair is statically named <Default-RSA-Key>.
modulus <i>size</i>	(Optional)	Specifies the modulus size of the key pair(s): 512, 768, 1024, and 2048. The default modulus size is 1024.
noconfirm	(Optional)	Suppresses all interactive prompting.
usage-keys	(Optional)	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:

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

Command History

Release	Modification
3.1(1)	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.

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	(Optional) Removes RSA key pairs with no labels. This keyword is legal only with RSA key pairs.
dsa	Specifies DSA as the key type.
label <i>key-pair-label</i>	(Optional) Removes the key pairs of the indicated type (rsa or dsa). If you do not provide a label, the FWSM removes all key pairs of the indicated type.
noconfirm	(Optional) 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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

Use the **crypto map interface** command in global configuration mode to apply a previously defined crypto map set to an interface. Use the **no** form of this command to remove the crypto map set from the interface.

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

Syntax Description

<i>interface-name</i>	Specifies the interface for the FWSM to use for establishing tunnels with VPN peers. If ISAKMP is enabled, and you are using a certificate authority to obtain certificates, this should be the interface with the address specified in the CA certificates.
<i>map-name</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use this command to assign a crypto map set to any active FWSM interface. The FWSM 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 FWSM evaluates the crypto map entry with the lowest *seq-num* first.

**Note**

The FWSM lets you change crypto map, dynamic map, and IPsec settings on the fly. If you do so, the FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM forms a security association using the configuration of that crypto map entry.

```
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.

[no] crypto map *map-name seq-num ipsec-isakmp dynamic dynamic-map-name*

Syntax Description

<i>dynamic-map-name</i>	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.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to remove the ipsec-manual keyword.

Usage Guidelines

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.

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 FWSM 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 FWSM 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. Use the **no** form of this command to remove the access list from a crypto map entry.

crypto map *map-name seq-num match address acl_name*

no crypto map *map-name seq-num match address acl_name*

Syntax Description

<i>acl_name</i>	Specifies the name of the encryption access list. This name should match the name argument of the named encryption access list being matched.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is required for all static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended. You would use the **access-list** command to define this access list.

IPSec uses this access list to differentiate the traffic to protect by IPSec crypto from the traffic that does not need protection. (Traffic permitted by the access list is protected. Traffic denied by the access list is not protected in the context of the corresponding crypto map entry.)



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 FWSM, the management address. Only tunnels to the FWSM 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	Indicates that this peer can only respond to inbound IKE connections for Site-to-Site connections based on this crypto map entry. It cannot originate connection requests. This keyword is the only available option for transparent firewall mode.
bidirectional	Indicates 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. This keyword is not available in transparent firewall mode.
map-name	Specifies the name of the crypto map set.
originate-only	Indicates that this peer can only originate connections based on this crypto map entry. It cannot accept inbound connections. This keyword is not available in transparent firewall mode.
seq-num	Specifies the number you assign to the crypto map entry.

Defaults

The default setting is bidirectional.

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
3.1(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, configures the crypto map mymap and sets the connection-type to bidirectional:

```
hostname(config)# crypto map mymap 10 set connection-type bidirectional
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 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 | hostname*10}

no crypto map *map-name seq-num set peer* {*ip_address | hostname*} {...*ip_address | hostname*10}

Syntax Description

<i>hostname</i>	Specifies a peer by its host name as defined by the FWSM name command.
<i>ip_address</i>	Specifies a peer by its IP address.
<i>map-name</i>	Specifies the name of the crypto map set.
peer	Specifies an IPSec peer in a crypto map entry either by hostname or IP address.
<i>seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	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.

For LAN-to-LAN connections, you can use multiple peers only with originator-only connection type. Configuring multiple peers is equivalent to providing a fallback list. For each tunnel, the FWSM attempts to negotiate with the first peer in the list. If that peer does not respond, the FWSM 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 is originate-only type).

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 perfect forward secrecy (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** | **group7**]

no crypto map *map-name seq-num set pfs* [**group1** | **group2** | **group5** | **group7**]

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.
group7	Specifies that IPSec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the MovianVPN client.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to add Diffie-Hellman group 7.

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 FWSM 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 FWSM assumes a default of group2. If the local configuration specifies group2, group5, or group7, that group must be part of the peer's offer or the negotiation fails.

For a negotiation to succeed PFS has to be set on both ends. If set, the groups have to be an exact match; The FWSM 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.

Diffie-Hellman Group 7 generates IPSec SA keys, where the elliptical curve field size is 163 bits. You can use this option with any encryption algorithm. This option is intended for use with the movianVPN client, but you can use it with any peers that support Group 7 (ECC).

When interacting with the Cisco VPN client, the FWSM 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 phase1mode** 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 FWSM uses group 2.

```
crypto map map-name seq-num set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}
```

```
no crypto map map-name seq-num set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}
```

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.
group7	Specifies that IPSec should use group7 (ECC) where the elliptical curve field size is 163-bits, for example, with the MovianVPN client.
main	Specifies main mode for phase one IKE negotiations.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 mymap 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 set reverse-route*

Syntax Description

<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM 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 the lifetime value of a crypto map entry 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

<i>kilobytes</i>	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.
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seconds</i>	Specifies the number of seconds a security association will live before it expires. The default is 28,800 seconds (eight hours).
<i>seq-num</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The security associations of a crypto map 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 FWSM 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 FWSM 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 FWSM lets you change crypto map, dynamic map, and ipsec settings on the fly. If you do so, the FWSM 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 with the crypto map entry, use the **crypto map set transform-set** command in global configuration mode. Use the **no** form of this command to remove the specified transform sets from a crypto map entry.

crypto map *map-name seq-num set transform-set transform-set-name1*
[... *transform-set-name9*]

no crypto map *map-name seq-num set transform-set transform-set-name1*
[... *transform-set-name9*]

Syntax Description

<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>transform-set-name1</i> <i>transform-set-name9</i>	Specifies the name(s) of the transform set(s), defined using the crypto ipsec transform-set command, to use for the crypto map. For an ipsec-isakmp or dynamic crypto map entry, you can specify up to nine transform sets.

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
1.1(1)	This command was introduced.

Usage Guidelines

This command is required for all crypto map entries.

If the local FWSM initiates the negotiation, the transform sets are presented to the peer in the order specified in the **crypto map** command statement. If the peer initiates the negotiation, the local FWSM accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec does not establish a security association. The traffic is dropped because there is no security association to protect the traffic.

If you want to change the list of transform sets, respecify the new list of transform sets to replace the old list. This change is applied only to **crypto map** command statements that reference this transform set.

Any transform sets included in a **crypto map** command statement must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example, entered in global configuration mode, specifies two transform sets (tfset1 and tfset2) for the crypto map mymap:

```
hostname(config)# crypto map mymap 10 set transform-set tfset1 tfset2
hostname(config)#
```

The following example, entered in global configuration mode, shows the minimum required crypto map configuration when the FWSM uses IKE to establish the security associations:

```
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
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
crypto ipsec transform-set	Configures a transform-set.
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. Use the **no** form of this command to remove a trustpoint from a crypto map entry.

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).
<i>map-name</i>	Specifies the name of the crypto map set.
<i>seq-num</i>	Specifies the number you assign to the crypto map entry.
<i>trustpoint-name</i>	Identifies the certificate to be sent during Phase 1 negotiations. The default is none.

Defaults

The default value is none.

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
3.1(1)	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.



CHAPTER

10

debug aaa through debug sip Commands

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** | **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.
internal	(Optional) Show debug messages for AAA functions supported by the local database only.
<i>level</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 acl optimization

To show debug messages for access list optimization, use the **debug acl optimization** command in privileged EXEC mode. To stop showing access list optimization messages, use the **no** form of this command.

debug optimization

no debug optimization

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
4.0(1)	This command was introduced.

Usage Guidelines

The **debug acl optimization** command displays detailed information about access list optimization activity. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables debugging for access list optimization functions:

```
hostname(config)# debug acl optimization
```

```
context 0 :: access-list test :: start time = 11:38:38, end time = 11:38:40, total time = 2.231 sec
```

Related Commands

Command	Description
access-list optimization enable	Enables access list optimization.
clear configure access-list	Clears an access list from the running configuration.
copy optimized-running-config	Copies the optimized running configuration to the designated location.

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

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 FWSM 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:

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

Command History

Release	Modification
3.1(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 debugs.

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:

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

Command History

Release	Modification
1.1(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 ARP:

```
hostname# debug arp
```

Related Commands

Command	Description
show debug	Shows all enabled debuggers.
arp	Adds a static ARP entry.
show arp statistics	Shows ARP statistics.

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:

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

Release	Modification
2.2(1)	This command was introduced.

Command History

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 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as debug pdm history).
3.1(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 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 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:

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

Command History

Release	Modification
2.2(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 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 context management:

```
hostname# debug context
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.

Command	Description
show context	Shows context information.
show debug	Shows all enabled debuggers.

debug control-plane

To show debug messages for the control plane, use the **debug control-plane** command in privileged EXEC mode. To stop showing debug messages for the control-plane, use the **no** form of this command.

debug control-plane { *egress* | *gc* | *ingress* | *tcp* | *tlv* | *udp* | *xlate* } [*level*]

no debug control-plane { *egress* | *gc* | *ingress* | *tcp* | *tlv* | *udp* | *xlate* } [*level*]

Syntax Description

egress	Shows debug messages related to packet egress processing.
gc	Shows garbage collection related debug messages.
ingress	Shows debug messages related to packet ingress processing.
<i>level</i>	(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.
tcp	Shows debug messages related to TCP connection, including SEQ and ACK numbers, window size, and TCP flags.
tlv	Shows debug messages related to TLV processing, and TLVs inserted into packets and their contents.
udp	Shows debug messages related to UDP, including the source and destination port numbers.
xlate	Shows debug messages related to NAT/PAT queries made to NPs, such as the type of query, parameters passed, and the values returned.

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
3.1(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 packets:

```
hostname# debug control-plane tcp
```

Related Commands

Command	Description
show debug	Shows all enabled debuggers.

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.
<i>level</i>	(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:

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

Command History

Release	Modification
1.1(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 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 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
1.1(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 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.
<i>level</i>	(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:

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

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
3.1(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 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 ctique	Enables CTIQBE application inspection.
show ctique	Displays information about CTIQBE sessions established through the FWSM.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug dhcpd

To enable debugging of the DHCP client, use the **debug dhcpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug dhcpd {detail | packet | error} [level]

no debug dhcpd {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.
<i>level</i>	(Optional) Specifies the debug level. Valid values 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

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 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 shows how to enable debugging for the DHCP client:

```
hostname# debug dhcpd detail 5
debug dhcpd 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.
<i>level</i>	(Optional) Specifies the debug level. Valid values 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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

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 **debug 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 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 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 dhcprelay

To enable debugging of the DHCP relay server, use the **debug dhcprelay** 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.
<i>level</i>	(Optional) Specifies the debug level. Valid values 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from debug .

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 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.
<i>level</i>	(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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1(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 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]

Syntax Description

all	(Default) Shows all messages, including messages about the DNS cache.
<i>level</i>	(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 FWSM shows all messages.

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
1.1(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 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:

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

Release	Modification
4.0(1)	This command was introduced.

Command History

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 first 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:

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

Command History

Release	Modification
4.0(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 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:

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

Command History

Release	Modification
4.0(1)	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:

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

Command History

Release	Modification
4.0(1)	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:

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

Release	Modification
4.0(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 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 management information base (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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(1)	Support for 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 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 {**onat** | **tcp** | **udp**} [*level*]

no debug fixup

Syntax Description

<i>level</i>	(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.
onat	Enables application inspection messages related to outside NAT.
tcp	Enables TCP-related application inspection messages.
udp	Enables UDP-related application inspection messages.

Defaults

All options are 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **debug fixup** command displays detailed information about application inspection. The **no debug all** or **undebug all** commands turn off all enabled debugs.

Examples

The following example enables the display of detailed TCP-related information:

```
hostname# debug fixup tcp
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.

Commands	Description
inspect <i>protocol</i>	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** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdump** | **rxip** | **switch** | **sync** | **tx** | **txdump** | **txip** | **verify** }

no debug fover { **cable** | **fail** | **fmsg** | **ifc** | **open** | **rx** | **rxdump** | **rxip** | **switch** | **sync** | **tx** | **txdump** | **txip** | **verify** }

Syntax Description

cable	Failover LAN status .
fail	Failover internal exception.
fmsg	Failover message.
ifc	Network interface status trace.
open	Failover device open.
rx	Failover message receive.
rxdump	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.
txdump	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(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 example shows how to display debug information for failover command replication:

```
hostname# debug fover sync  
fover event trace on
```

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:

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

Command History

Release	Modification
3.1(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 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:

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

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
3.1(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 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	(Optional) Displays debug information on errors encountered while processing the GTP message.
event	(Optional) Displays debug information on GTP events.
ha	(Optional) Debugs information on GTP HA events.
parser	(Optional) 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:

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

Command History

Release	Modification
3.1(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 debugs.



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 {gup | h225 | h245 | ras} [asn | event]

no debug h323 {gup | h225 | h245 | ras} [asn | event]

Syntax Description

asn	(Optional) Displays the output of the decoded PDUs.
event	(Optional) Displays the events of the H.245 signaling or turns on both traces.
gup	Specifies GUP signaling.
h225	Specifies H.225 signaling.
h245	Specifies H.245 signaling.
ras	Specifies the registration, admission, and status protocol.

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
1.1(1)	This command was introduced.
3.2(1)	The keyword gup 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.



Note

Enabling the **debug h323** command may slow down traffic on busy networks.

Examples

The following is sample output when debug messages are enabled 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 FWSM.
show h245	Displays information for H.245 sessions established across the FWSM by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
timeout (gtp-map)	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	<i>level</i>	(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 for *level* is 1.

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
	3.1(1)	Support for 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 debugs.

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 FWSM.
	http-proxy	Configures an HTTP proxy server.
	http server enable	Enables the FWSM 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:

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

Command History

Release	Modification
3.1(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	trace	Displays debug information about ICMP trace activity.
	<i>level</i>	(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 All options are enabled.

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
	3.1(1)	Support for 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 FWSM interface.
	show conn	Displays the state of connections through the FWSM 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 <i>group_id</i>	Displays IGMP debug information for the specified group.
interface <i>if_name</i>	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:

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

Command History

Release	Modification
3.1(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 CiscoTAC. 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 FWSM 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:

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

Command History

Release	Modification
1.1(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 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.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(1)	Support for 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 ip bgp

To display debug information for the BGP routing processes, use the **debug ip bgp** command in privileged EXEC mode.

debug ip bgp

no debug ip bgp

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 ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

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 bgp** command:

```
hostname# debug ip bgp
```

Related Commands

Command	Description
show ip bgp summary	Displays general information about the BGP routing process.

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:

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

Command History

Release	Modification
3.1(1)	Support for 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 | 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.
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
3.1(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 from 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 an FWSM 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 individual user authentication (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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(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 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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
2.2(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 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 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.
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 technical support staff.

Syntax Description

This command should be used only under the supervision of Cisco technical support staff.

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
3.1(1)	Support for 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

This command should be used only under the supervision of Cisco technical support staff.

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 | mrrib | pak | ps | signal} [*group*]

no debug mfib {db | init | mrrib | pak | ps | signal} [*group*]

Syntax Description

db	(Optional) Displays debug information for route database operations.
<i>group</i>	(Optional) IP address of the multicast group.
init	(Optional) Displays system initialization activity.
mrrib	(Optional) Displays debug information for communication with MRIB.
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:

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

Command History

Release	Modification
3.1(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 database 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:

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

Command History

Release	Modification
2.2(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 FWSM.
show conn	Displays the connection state for different connection types.

debug mrrib

To display MRIB debug information, use the **debug mrrib** command in privileged EXEC mode. To stop the display of debug information, use the **no** form of this command.

debug mrrib { **client** | **io** | **route** [*group*] | **table** }

no debug mrrib { **client** | **io** | **route** [*group*] | **table** }

Syntax Description

client	Enables debugging for MRIB client management activity.
<i>group</i>	Enables debugging of MRIB routing entry activity for the specified group.
io	Enables debugging of MRIB I/O events.
route	Enables debugging of MRIB routing entry activity.
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:

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

Command History

Release	Modification
3.1(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 CiscoTAC. 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 mrrib 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 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:

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

Command History

Release	Modification
3.1(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 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 ospf

To display debug information about the OSPF routing processes, use the **debug ospf** command in privileged EXEC mode.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
3.1(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 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 pim

To display PIM 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 <i>group</i>	(Optional) Displays debug information for the specified group. The value for <i>group</i> 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 <i>if_name</i>	(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 <i>rp</i>	(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:

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

Command History	Release	Modification
	3.1(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 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 pim command:

```

hostname# debug pim
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received Join/Prune on Vlan101 from 172.24.37.33
PIM: Received RP-Reachable on Vlan101 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 Vlan101 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 Vlan101
PIM: Received Join/Prune on Vlan101 from 172.24.37.6
PIM: Received Join/Prune on Vlan101 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 Vlan101 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 (Vlan101)

```

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:

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

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
1.1(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 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:

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

Release	Modification
1.1(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 debug messages for xlate and secondary connections processing:

```
hostname# debug pix process
```

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:

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

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
3.1(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 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.
<i>username</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **debug radius** command displays detailed information about RADIUS messaging between the FWSM 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 FWSM.

debug route-inject

To enable debugging of the route-injections that have been configured on FWSM, use the **debug route-inject** command in global configuration mode.

debug route-inject

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
Global configuration	•	—	•	•	—

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines The **debug route-inject** command allows you debug the route-injections that have been configured on FWSM.

Examples The following is sample output from the **debug route-inject** command:

```
hostname(config)# debug route-inject
hostname(config)# route-inject
hostname(config-route-inject)# redistribute connected interface blah31
route_inject_walk_routes_type: operation inject, context single_vf (0), type connected
checking: ip 10.94.180.0, mask 255.255.255.0, gw 10.94.180.35, proto 15, weight 1, vlan
31, SysIP 31.1.1.1
hostname(config-route-inject)# match 1, injected 0, send_update 1, advertise 1
add: ip 10.94.180.0, mask 255.255.255.0, gw 10.94.180.35, proto 15, weight 1, vlan 31,
SysIP 31.1.1.1 checking: ip 20.1.1.0, mask 255.255.255.0, gw 20.1.1.1, proto 15, weight 1,
vlan 31, SysIP 31.1.1.1 operation inject, match 1, injected 0, send_update 1, advertise 1
add: ip 20.1.1.0, mask 255.255.255.0, gw 20.1.1.1, proto 15, weight 1, vlan 31, SysIP
31.1.1.1
FWSM(config-route-inject)#
```

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
redistribute	Configures the type of route or NAT pools to inject.
route-inject	Injects the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.
show route-inject	Displays the routes and NAT pools that have been injected.
show running-config route-inject	Displays the route-injection running configuration.

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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(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 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:

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

Command History

Release	Modification
3.1(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 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 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 [*level*]

no debug sip [*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:

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

Command History

Release	Modification
1.1(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 sip** command may slow down traffic on busy networks.

Examples

The following example enables debug messages at the default level (1) for SIP application inspection:

```
hostname# debug sip
```

Related Commands

Command	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sip	Enables SIP application inspection.

Command	Description
show conn	Displays the connection state for different connection types.
show sip	Displays information about SIP sessions established through the FWSM.
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:

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

Command History

Release	Modification
1.1(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 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 FWSM.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

debug smtp

To show debug messages for SMTP/ESMTP application inspection, use the **debug smtp** command in privileged EXEC mode. To stop showing debug messages for SMTP/ESMTP application inspection, use the **no** form of this command.

debug smtp [*level*]

no debug smtp [*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:

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

Command History

Release	Modification
1.1(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 smtp** 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 smtp
```

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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(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 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:

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

Command History

Release	Modification
1.1(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 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 FWSM.
ssh	Allows SSH connectivity to the FWSM 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(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 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 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.
<i>username</i>	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:

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

Command History

Release	Modification
1.1(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 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 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:

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

Command History

Release	Modification
3.1(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:

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

Command History

Release	Modification
3.1(1)	Support for 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 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 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:

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

Command History

Release	Modification
3.1(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 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.



CHAPTER

11

default through drop 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:

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

Release	Modification
3.1(1)	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 (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:

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

Command History

Release	Modification
3.1(1)	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 FWSM; 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 FWSM based on time.

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:

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

Command History	Release	Modification
	3.1(1)	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
```

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 <i>domain-name</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can use only alphanumeric characters, hyphens (-), and periods (.) in default domain names.

To delete all default domain names, use the **no** form of this command without arguments. This deletes all configured default domain names, including a null list created by issuing the **default-domain none** command.

To prevent users from inheriting a domain name, use the **default-domain none** command.

The FWSM 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.

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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The default group policy DfltGrpPolicy comes with the initial configuration of the FWSM. 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-general)# default-group-policy first-policy
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-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-map default group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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

<i>acl-name</i>	(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:

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

Command History

Release	Modification
4.0(1)	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

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 <i>value</i>	(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 <i>name</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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-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

<i>bandwidth</i>	The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
<i>delay</i>	The route delay in tens of microseconds. Valid values are 1 to 4294967295.
<i>reliability</i>	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.
<i>loading</i>	The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
<i>mtu</i>	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:

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

Command History

Release	Modification
4.0(1)	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

<i>delay-time</i>	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:

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

Command History

Release	Modification
4.0(1)	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)# show interface outside
Interface Vlan20 "outside", is up, line protocol is up
Hardware is EtherSVI, BW Unknown Speed-Capability, DLY 10 usec
MAC address 000f.23be.d980, MTU 1500
IP address 20.1.1.1, subnet mask 255.255.255.0
Traffic Statistics for "outside":
0 packets input, 0 bytes
```

 delay

```
0 packets output, 0 bytes
0 packets dropped
FWSM(config-if)#
```

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] [disk:]*filename*

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
/recursive	(Optional) Deletes the specified file recursively in all subdirectories.
<i>filename</i>	Specifies the name of the file to delete.
disk:	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
2.2(1)	This command was introduced.

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

To deny traffic based on the application type, use the **deny** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. The Programmable Intelligent Services Accelerator (PISA) on the switch can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type. To remove the deny statement, use the **no** form of this command.

deny {**all** | *protocol*}

no deny {**all** | *protocol*}

Syntax Description

all	Specifies all protocols.
<i>protocol</i>	Specifies a specific protocol, by name or number. For a list of supported protocol names, use the deny ? command.

Defaults

By default, all protocols are permitted unless you specifically deny them.

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
4.0(1)	This command was introduced.

Usage Guidelines

Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags using GRE can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to configure multiple upstream switches with PISAs installed.

You might want to deny certain types of application traffic when you want to preserve bandwidth for critical application types. For example, you might deny the use of peer-to-peer (P2P) applications if they are affecting your other critical applications.

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **deny** command (along with **permit** commands) to determine the traffic to deny.

Like access lists, you can combine **permit** and **deny** statements to narrow the traffic that you want denied. By default, all traffic is permitted.

For example, to permit all traffic except for Skype, eDonkey, and Yahoo, enter the following commands:

```
hostname(config-pmap-c) # deny skype
hostname(config-pmap-c) # deny yahoo
hostname(config-pmap-c) # deny eDonkey
```

The following example denies all traffic except for Kazaa and eDonkey:

```
hostname(config-pmap-c) # deny all
hostname(config-pmap-c) # permit kazaa
hostname(config-pmap-c) # permit eDonkey
```

See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for detailed information about PISA integration, including essential information about configuring the switch to work with this feature.

Examples

The following is an example configuration for PISA integration:

```
hostname(config) # access-list BAD_APPS extended permit 10.1.1.0 255.255.255.0 10.2.1.0
255.255.255.0

hostname(config) # class-map denied_apps
hostname(config-cmap) # description "Apps to be blocked"
hostname(config-cmap) # match access-list BAD_APPS

hostname(config-cmap) # policy-map denied_apps_policy
hostname(config-pmap) # class denied_apps
hostname(config-pmap-c) # deny skype
hostname(config-pmap-c) # deny yahoo
hostname(config-pmap-c) # deny eDonkey

hostname(config-pmap-c) # service-policy denied_apps_policy inside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
permit	Permits PISA-tagged traffic.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
show conn	Shows connection information.

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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	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), use the **description** command in various configuration modes. To remove the description, use the **no** form of this command. The description adds helpful notes in your configuration.

description *text*

no description

Syntax Description

<i>text</i>	Sets the description as a text string up to 200 characters in length. 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
1.1(1)	This command was introduced.

Examples

The following example adds a description to the “Administration” context configuration:

```
hostname(config)# context administrator
hostname(config-ctx)# description This is the admin context.
hostname(config-ctx)# allocate-interface vlan 100
hostname(config-ctx)# allocate-interface vlan 200
hostname(config-ctx)# config-url disk://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.
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.

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*

Syntax Description

<i>interface_name</i>	Interface the address pool is assigned to.
<i>IP_address1</i>	Start address of the DHCP address pool.
<i>IP_address2</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd address** *ip1*[-*ip2*] *interface_name* command specifies the DHCP server address pool. The address pool of a FWSM DHCP server must be within the same subnet of the FWSM interface on which it is enabled, and you must specify the associated FWSM interface using *interface_name*.

The size of the address pool is limited to 256 addresses per pool on the FWSM. If the address pool range is larger than 253 addresses, the netmask of the FWSM 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 FWSM DHCP 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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for information on how to implement the DHCP server feature into the FWSM.

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 FWSM:

```
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 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*]

no dhcpd dns [*dnsip1* [*dnsip2*]]

Syntax Description

<i>dnsip1</i>	IP address of the primary DNS server for the DHCP client.
<i>dnsip2</i>	(Optional) IP address of the alternate DNS server for the DHCP client.

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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

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 FWSM.

```
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*

no dhcpd domain [*domain_name*]

Syntax Description

domain_name The DNS domain name, for example example.com.

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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

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 FWSM:

```
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 FWSM means that the FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

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 FWSM 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 FWSM DHCP server daemon does not support clients that are not directly connected to a FWSM interface.

Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for information on how to implement the DHCP server feature into the FWSM.

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*

no dhcpd lease [*lease_length*]

Syntax Description

<i>lease_length</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

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. You can use the **dhcpd option** command to provide TFTP server information to Cisco IP Phones and routers.

dhcpd option *code* { **ascii** *string* } | { **ip** *IP_address* [*IP_address*] } | { **hex** *hex_string* }

no dhcpd option *code*

Syntax Description

ascii	Specifies that the option parameter is an ASCII character string.
<i>code</i>	A number representing the DHCP option being set. Valid values are 0 to 255. See the “Usage Guidelines” section, below, for the list of DHCP option codes that are not supported.
hex	Specifies that the option parameter is a hexadecimal string.
<i>hex_string</i>	Specifies a hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
ip	Specifies that the option parameter is an IP address. You can specify a maximum of two IP addresses with the ip keyword.
<i>IP_address</i>	Specifies a dotted-decimal IP address.
<i>string</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

When a DHCP option request arrives at the FWSM DHCP server, the FWSM 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 RFC 2132.

**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
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*

no dhcpd ping-timeout

Syntax Description

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The FWSM 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 FWSM 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 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*]

no dhcpd wins [*server1* [*server2*]]

Syntax Description

<i>server1</i>	Specifies the IP address of the primary Microsoft NetBIOS name server (WINS server).
<i>server2</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

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.

dhcp-network-scope

To specify the range of IP addresses the FWSM 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

<i>ip_address</i>	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:

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

Command History

Release	Modification
3.1(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 FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

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 FWSM interface to a specified DHCP server.

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

Syntax Description

<i>interface_name</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

For the FWSM 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 FWSM 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 DHCP 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 FWSM, client requests on the inside interface of the FWSM, 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 information trust

You can preserve option 82 and forward a packet by identifying an interface as a trusted interface thus ensuring that DHCP snooping and IP source guard features on the switch work along with the FWSM.

You can enable this feature on interfaces configured with IPv4 and IPv6 addresses.

To configure a particular interface as a trusted interface that preserves option 82, enter the following command:

```
dhcprelay information trusted
```

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
4.0	This command was introduced.

Usage Guidelines

The interface-specific trusted configuration and global trusted configuration can exist together. For example there are three interfaces A, B and C, and a user configures interface A as trusted using the interface-specific command. Then the user configures the global command also.

Now all the three interfaces A, B, and C are trusted interfaces. If you enter the no dhcprelay information trust-all command, then interfaces B and C will become non-trusted interfaces. Interface A will continue to be a trusted interface, since the interface-specific trusted configuration is not removed.

Examples

The following example enables a particular interface as a trusted interface:

```
hostname(config)# dhcprelay information trusted
```

Related Commands

Command	Description
dhcprelay information trust-all	To configure all interfaces as trusted interfaces.

dhcprelay information trust-all

You can preserve option 82 and forward packets by identifying all the interfaces as trusted interfaces and ensuring that DHCP snooping and IP source guard features on the switch work along with the FWSM.

You can enable this feature on interfaces configured with IPv4 and IPv6 addresses.

To configure all interfaces as trusted interfaces, enter the following command:

dhcprelay information trust-all

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
Global configuration	•	—	•	•	—

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The interface-specific trusted configuration and global trusted configuration can exist together. For example there are three interfaces A, B and C, and a user configures interface A as trusted using the interface-specific command. Then the user configures the global command also.

Now all the three interfaces A, B, and C are trusted interfaces. If you enter the no dhcprelay information trust-all command, then interfaces B and C will become non-trusted interfaces. Interface A will continue to be a trusted interface, since the interface-specific trusted configuration is not removed.

Examples

The following example enables all interfaces except the interfaces that are shared or configured for the DHCP server:

```
hostname(config)# dhcprelay information trust-all
```

Related Commands

Command	Description
dhcprelay information trusted	To configure specific interfaces as trusted interfaces.

dhcprelay server

To specify the DHCP server that DHCP requests are forwarded to, use the **dhcprelay 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 FWSM interface to a specified DHCP server.

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address [interface_name]*

Syntax Description

<i>interface_name</i>	Name of the FWSM interface on which the DHCP server resides.
<i>IP_address</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

You can add up to four DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the FWSM 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. If there is **no dhcprelay enable** command in the configuration, then the sockets are not opened and the DHCP relay task does not start.

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 FWSM, client requests on the inside interface of the FWSM, 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 FWSM 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

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 FWSM adds one containing the address of *interface*. This action allows the client to set its default route to point to the FWSM.

When you do not configure the **dhcprelay setroute** *interface* command (and there is a default router option in the packet), it passes through the FWSM 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 FWSM:

```
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

<i>seconds</i>	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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

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 FWSM, client requests on the inside interface of the FWSM, 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.

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 *hostname1* [...*hostname10*]

no dhcp-server *hostname*

In interface level, enter the **dhcp-server** <ip_address> command. There is no need to add <interface> in the command.

Syntax Description

<i>hostname1</i>	Specifies the IP address of the DHCP server. You can specify up to 10
<i>...hostname10</i>	DHCP servers.

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
Tunnel-group general attributes configuration	•		•		

Command History

Release	Modification
3.1(1)	This command was introduced.

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-general)# default-group-policy remotegrp
hostname(config-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-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-map default group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

dir

To display the directory contents, use the **dir** command in privileged EXEC mode.

dir [/all] [all-file systems] [/recursive] [flash: | system:] [path]

Syntax Description

/all	(Optional) Displays all files.
all-file systems	(Optional) Displays the files of all file systems
/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:

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

Command History

Release	Modification
3.1(1)	Support for 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)
```

This 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:

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines Use the **enable** command to enter privileged EXEC mode. The **disable** command lets you exit privileged EXEC mode and returns you to user EXEC mode.

Examples The following example shows how to enter privileged EXEC mode:

```
hostname> enable
hostname#
```

The following example shows how to exit privileged EXEC mode:

```
hostname# disable
hostname>
```

Command	Description
enable	Enables privileged EXEC mode.

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

<i>external-distance</i>	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.
<i>internal-distance</i>	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:

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

Command History

Release	Modification
4.0(1)	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 FWSM 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 FWSM, 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 FWSM.

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

<i>d1</i> , <i>d2</i> , and <i>d3</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 reenter 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

<i>acl</i>	Name of a standard access list.
<i>if_name</i>	(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		
	Routed	Transparent	Single	Multiple Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(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 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.

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.

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* | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name* | **ospf** *pid* | **static** | **connected**]

Syntax Description

<i>acl</i>	Name of a standard access list.
connected	(Optional) Filters only connected routes.
interface <i>if_name</i>	(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 <i>pid</i>	(Optional) Filters only OSPF routes discovered by the specified OSPF process.
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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If no interface is specified, the access list will be applied to all outgoing updates.

Examples

The following example filters only OSPF routes discovered by the specified OSPF process on the outside interface:

```
hostname(config)# access-list ospf 100
hostname(config)# router ospf 100
hostname(config-router)# distribute-list ospf_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.
show running-config router	Displays the commands in the global router configuration.

dns domain-lookup

To enable the FWSM 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 FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM caches information returned from external DNS requests. The FWSM 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 FWSM 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 name-server

To identify one or more DNS servers, use the **dns name-server** command in global configuration mode. To remove a server, use the **no** form of this command. The FWSM uses DNS to resolve server names in your certificate configuration (see the 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.

[no] dns 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 FWSM saves each server in a separate command in the configuration. The FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To enable DNS lookup, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used.

Commands that support DNS resolution include the following:

- **enrollment url**
- **url**

You can manually enter names and IP addresses using the **name** command.

See the **dns retries** command to set how many times the FWSM tries the list of DNS servers.

Examples

The following example adds three DNS servers:

```
hostname(config)# dns name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

The FWSM saves the configuration as separate commands, as follows:

```
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
```

To add two additional servers, you can enter them as one command:

```
hostname(config-if)# dns name-server 10.5.1.1 10.8.3.8
hostname(config-if)# show running-config dns
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
dns name-server 10.5.1.1
dns name-server 10.8.3.8
...
```

Or you can enter them as two commands:

```
hostname(config)# dns name-server 10.5.1.1
hostname(config)# dns 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)# no dns name-server 10.5.1.1 10.8.3.8
```

Related Commands

Command	Description
dns domain-lookup	Enables the FWSM to perform a name lookup.
dns retries	Specifies the number of times to retry the list of DNS servers when the FWSM 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 retries

To specify the number of times to retry the list of DNS servers when the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Add DNS servers using the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The FWSM only tries each server one time.

```
hostname(config)# dns retries 0
```

Related Commands

Command	Description
dns domain-lookup	Enables the FWSM 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.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

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 FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM does not receive a response.
dns domain-lookup	Enables the FWSM to perform a name lookup.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns-guard

To <text>, use the **dns-guard** command in global configuration mode.

To <text about removing command>, use the **no** form of this command.

dns-guard

no dns-guard

Syntax Description

There are no arguments or keywords for this command.

Defaults

DNS Guard 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When a client sends a DNS request to an external DNS server, only the first response is accepted by the FWSM. All additional responses from other DNS servers are dropped by the FWSM.

After the client issues a DNS request, a dynamic hole allows UDP packets to return from the DNS server. When the FWSM receives a response from the first DNS server, the connection that was created in the accelerated path is dropped so that subsequent responses from other DNS servers are dropped by the FWSM. The UDP DNS connection is deleted immediately rather than marking the connection for deletion.

The FWSM creates a session-lookup key based on the source and destination IP address along with the protocol and the DNS ID instead of the source and destination ports.

If the DNS client and DNS server use TCP for DNS, the connection is cleared like a normal TCP connection.

However, if clients receive DNS responses from multiple DNS servers, you can disable the default DNS behavior on a per context basis. When DNS Guard is disabled, a response from the first DNS server does not delete the connection and the connection is treated as a normal UDP connection.

Examples

The following example shows the use of the **dns-guard** command to disable the DNS Guard feature:

```
hostname(config)# no dns-guard
```

```
hostname(config)# show running-config | inc dns-guard
no dns-guard
hostname(config)#
```

Related Commands

Command	Description
inspect dns	Enables inspection of DNS application traffic.

dns-server

To set the IP address of the primary and secondary DNS servers, use the **dns-server** command in group-policy mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a DNS server from another group policy. To prevent inheriting a server, use the **dns-server none** 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 <i>ip_address</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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
```


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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM to perform a name lookup.
dns name-server	Configures a DNS server address.

Command	Description
hostname	Sets the FWSM hostname.
show running-config domain-name	Shows the domain name configuration.

drop (class)

To drop all packets that match the **match** command or **class** command, use the **drop** command in match or class configuration mode. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. To disable this action, use the **no** form of this command.

drop [log]

no drop [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:

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

Command History

Release	Modification
4.0(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 (gtp-map)

To drop specified GTP messages, use the **drop** command in gtp-map configuration mode. Use the **no** form to remove the command.

drop {**apn** *access_point_name* | **message** *message_id* | **version** *version*}

no drop {**apn** *access_point_name* | **message** *message_id* | **version** *version*}

Syntax Description

apn	Drops GTP messages with the specified access point name.
<i>access_point_name</i>	The text string of the APN which will be dropped.
message	Drops specific GTP messages.
<i>message_id</i>	An alphanumeric identifier for the message that you want to drop. The valid range for <i>message_id</i> is 1 to 255.
version	Drops GTP messages with the specified version.
<i>version</i>	Use 0 to identify Version 0 and 1 to identify Version 1. Version 0 of GTP uses port 2123, while Version 1 uses port 3386.

Defaults

All messages with valid message IDs, APNs, and version are inspected.
Any APN is allowed.

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
Gtp-map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **drop message** command to drop specific GTP messages that you do not want to allow in your network.

Use the **drop apn** command to drop GTP messages with the specified access point. Use the **drop version** command to drop GTP messages with the specified version.

Examples

The following example drops traffic to message ID 20:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# drop message 20
```

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.

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. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. The connection will be removed from the connection database on the FWSM. Any subsequent packets entering the FWSM for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map for application traffic; however, not all applications allow this action. To disable this action, use the **no** form of this command.

drop-connection [**log**]

no drop-connection [**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:

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

Command History

Release	Modification
4.0(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.



CHAPTER

12

eigrp log-neighbor-changes through ftp-map 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:

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

Release	Modification
4.0(1)	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
```

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:

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

Command History

Release	Modification
4.0(1)	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 FWSM is used as the router ID.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If the **eigrp router-id** command is not configured, EIGRP automatically selects the highest IP address on the FWSM 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 FWSM 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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Use the **eigrp stub** command to configure the FWSM as a stub where the FWSM directs all IP traffic to a distribution router.

Using the **receive-only** keyword restricts the FWSM from sharing any of its routes with any other router in the autonomous system; the FWSM 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. 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 not configure this option, EIGRP does not advertise redistributed routes.

Examples

The following example uses the **eigrp stub** command to configure the FWSM 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 FWSM 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 FWSM 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 FWSM 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 arguments, the **eigrp stub** commands advertises connected and summary 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.

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 the command.

email *address*

no email [*address*]

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the email address jjh@nhf.net in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# email jjh@nhf.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) Enters the privilege level between 0 and 15.

Defaults

Enters privilege level 15 unless you are using command authorization, 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The default enable password is blank. See the **enable password** command to set the password.

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.

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 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 FWSM 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 <i>level</i>	(Optional) Sets a password for a privilege level between 0 and 15.
<i>password</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM:

```
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 associate endpoints with an HSI group, use the **endpoint** command in HSI group configuration mode. To remove the endpoint, use the **no** form of this command.

endpoint *ip address interface*

no endpoint *ip address interface*

Syntax Description

<i>ip address</i>	The IP address of the endpoint.
<i>interface</i>	The interface on the FWSM that is connected to the endpoint.

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
HSI group configuration	•	•	•	•	—

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

Use the **endpoint** command to identify the endpoints associated with an HSI group. An HSI group allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling.

Each HSI group can contain a maximum of ten endpoints. You must configure an HSI within the group before configuring any endpoints. You must remove all endpoints and the HSI before removing the HSI group.

Examples

The following example shows how to define an H.225 map.

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
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
hostname(config-h225-map-hsi-grp)# exit
hostname(config-h225-map-hsi-grp)# exit
```

Related Commands	Commands	Description
	hsi	Defines the HSI associated with an HSI group.
	hsi-group	Defines an HSI group and enables HSI group configuration mode.
	h225-map	Defines an H.225 map and enables H.225 map configuration mode.
	inspect h323 h225	Applies an H.225 map to H.323 application inspection.

endpoint-mapper

To configure endpoint mapper options for DCERPC inspection, use the **endpoint-mapper** command in dcerpc-map 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 endpoint mapper service during binding.
lookup-operation	Specifies to enable lookup operation of the endpoint mapper service.
timeout <i>value</i>	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:

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

Command History

Release	Modification
3.2(1)	This command was introduced.

Examples

The following example shows how to configure the endpoint mapper in a DCERPC map:

```
hostname(config)# dcerpc_map dmap
hostname(config-dcerpc-map)# endpoint-mapper epm-service-only
```

Related Commands

Command	Description
clear configure dcerpc-map	Clears DCERPC map configuration.
show running-config dcerpc-map	Display all current DCERPC map configurations.
timeout pinhole	Configures the timeout for DCERPC pinholes and overrides the global system pinhole timeout.

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in `crl` configure configuration mode. If set, this command requires CRLs to have a NextUpdate field that has not yet lapsed. If not used, the FWSM allows a missing or lapsed NextUpdate field in a CRL.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters `crl` configure 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 <code>ca-crl</code> configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

enrollment retry count

To specify a retry count, use the **enrollment retry count** command in crypto ca trustpoint configuration mode. To restore the default setting of the retry count, use the **no** form of the command. After requesting a certificate, the FWSM waits to receive a certificate from the CA. If the FWSM does not receive a certificate within the configured retry period, it sends another certificate request. The FWSM repeats the request until either it receives a response or reaches the end of the configured retry period.

enrollment retry count *number*

no enrollment retry count

Syntax Description

number Sets 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:

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

Command History

Release	Modification
3.1(1)	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. To restore the default setting of the retry period, use the **no** form of the command. After requesting a certificate, the FWSM waits to receive a certificate from the CA. If the FWSM does not receive a certificate within the specified retry period, it sends another certificate request.

enrollment retry period *minutes*

no enrollment retry period

Syntax Description

minutes Sets 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:

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

Command History

Release	Modification
3.1(1)	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:

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

Command History

Release	Modification
3.1(1)	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

<i>url</i>	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:

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

Command History

Release	Modification
3.1(1)	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.

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 [flash:]

Syntax Description

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.

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
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

The **erase** command erases all data on the Flash memory using the 0xFF 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.

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.

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

<i>est_protocol</i>	Specifies the IP protocol (UDP or TCP) to use for the established connection lookup.
<i>dest_port</i>	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.
<i>port [-port]</i>	(Optional) Specifies the (UDP or TCP) destination port(s) of the return connection.
<i>protocol</i>	(Optional) IP protocol (UDP or TCP) used by the return connection.
<i>source_port</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(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 FWSM. This command works with an original connection that is outbound from a network and protected by the FWSM 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 FWSM supports XDMCP with assistance from the **established** command.

**Caution**

Using XWindows system applications through the FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM. 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.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(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. Any usernames, passwords, and preshared keys configured on the FWSM are transmitted in clear text and could pose a significant security risk. We recommend securing the failover communication with a failover key.

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 FWSM or failover group to the active state, use the **failover active** command in privileged EXEC mode. To switch an active FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM from a failed state to standby.

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:

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

Command History

Release	Modification
3.1(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**, 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**, and **failover replication http** commands have no effect in Active/Active failover configurations. They are overridden by the following failover group configuration mode commands: **polltime interface**, **interface-policy**, and **replication http**.

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.

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.
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

<i>if_name</i>	Interface name for the failover or Stateful Failover interface.
<i>ip_address mask</i>	Specifies the IP address and mask for the failover or Stateful Failover interface on the primary module.
standby <i>ip_address</i>	Specifies the IP address used by the secondary module to communicate with the primary module.

Defaults

Not configured.

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
2.2(1)	This command was introduced.

Usage Guidelines

Failover and Stateful Failover interfaces are functions of Layer 3, even when the FWSM 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 FWSM 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

<i>num</i>	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.
<i>%</i>	(Optional) Specifies that the number <i>num</i> 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:

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

Command History

Release	Modification
2.2(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 FWSM is functioning properly, the FWSM will mark itself as failed and a failover may occur (if the active FWSM 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 shared secret, use the **no** form of this command.

failover key {*secret* | **hex** *key*}

no failover key

Syntax Description

hex <i>key</i>	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0-9, a-f).
<i>secret</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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.



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. Any usernames, passwords, and preshared keys configured on the FWSM are transmitted in clear text and could pose a significant security risk. We recommend securing the failover communication with a failover key.

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 interface

To specify the interface name and VLAN 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 vlan vlan

no failover lan interface if_name vlan vlan
```

Syntax Description	<i>if_name</i>	Specifies the name of the FWSM interface dedicated to failover.
	vlan <i>vlan</i>	Specifies the VLAN number.

Defaults	Not configured.

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
	1.1(1)	This command was introduced.

Usage Guidelines

The active and standby modules constantly communicate over this link to determine the operating status of each module. Communications over the failover link include the the module state (active or standby), hello messages (also sent on all other interfaces), and configuration synchronization between the two modules.

Failover requires a dedicated interface for passing failover traffic, however you can also use the LAN failover interface for the Stateful Failover link. If you use the same interface for both LAN failover and Stateful Failover, the interface needs enough capacity to handle both the failover and Stateful Failover traffic.

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.

You can use any unused interface on the module 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).

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 an FWSM for failover.

Examples

The following example configures the failover LAN interface:

```
hostname(config)# failover lan interface folink vlan 101
```

Related Commands

Command	Description
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 FWSM as either the primary or secondary unit in a 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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 an FWSM for failover.

Examples

The following example sets the FWSM as the primary unit:

```
hostname(config)# failover lan unit primary
```

Related Commands

Command	Description
failover lan interface	Specifies the interface used for failover communication.

failover link

To specify the Stateful Failover interface and VLAN, 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* [**vlan** *vlan*]

no failover link

Syntax Description

<i>if_name</i>	Specifies the name of the FWSM interface dedicated to Stateful Failover.
vlan <i>vlan</i>	(Optional) Sets the VLAN used for stateful update information. If the Stateful Failover interface is sharing the interface assigned for failover communication, then this argument is not required.

Defaults

Not configured.

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
1.1(1)	This command was introduced.

Usage Guidelines

The physical or logical interface argument is required when not sharing the failover communication interface.

The **failover link** command enables Stateful Failover. Enter the **no failover link** command to disable Stateful Failover and also clear the Stateful Failover interface IP address configuration.

To use Stateful Failover, you must configure a state link to pass all state information. You have two options for configuring a state link: you can use a dedicated interface for the state link or you can use the failover link.



Caution

Sharing the Stateful Failover link with a regular firewall interface is not supported. This restriction was not enforced in previous versions of the software. If you are upgrading from a previous version of the FWSM software, and have a configuration that shares the state link with a regular firewall interface, then the configuration related to the firewall interface will be lost when you upgrade. To prevent your configuration from being lost, move the state link to a separate physical interface or disable Stateful Failover before upgrading.

The state traffic can be large. If you are using the failover link as the state link and you experience performance problems, consider dedicating a separate link for the state traffic.

In multiple context mode, the state 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 state link do not change at 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. Any usernames, passwords, and preshared keys configured on the FWSM are transmitted in clear text and could pose a significant security risk. We recommend securing the failover communication with a failover key.

Examples

The following example shows how to specify the Stateful Failover interface:

```
hostname(config)# failover link stateful_if vlan 101
```

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.
mtu	Specifies the maximum transmission unit for an interface.

failover polltime

To specify the failover unit and interface poll times and unit hold time, use the **failover polltime** command in global configuration mode. To restore the default poll time, use the **no** form of this command.

failover polltime [**unit**] [**msec**] *time* [**holdtime** *time*]

failover polltime interface *time*

no failover polltime [**unit**] [**msec**] *time* [**holdtime** *time*]

no failover polltime interface *time*

Syntax Description

holdtime <i>time</i>	(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 range from 3 to 45 seconds.
interface <i>time</i>	Specifies the poll time for interface monitoring. Valid values range from 3 to 15 seconds.
msec	(Optional) Specifies that the time interval between messages is in milliseconds. Valid values are from 500 to 999 milliseconds.
time	Amount of time between hello messages. The maximum value is 15 seconds.
unit	(Optional) Sets how often hello messages are sent on the failover link.

Defaults

The defaults are as follows:

- The **unit** poll *time* is 1 second.
- The **holdtime** *time* is 15 seconds.
- The **interface** poll *time* is 15 seconds.

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
1.1(1)	This command was introduced.
2.2(1)	This command was changed from the failover poll command to the failover polltime command and now includes unit , interface , and holdtime keywords.

Usage Guidelines

You cannot enter a **holdtime** value that is less than 3 times the unit poll time. With a faster poll time, the FWSM can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

When the **unit** or **interface** keywords are not specified, the poll time configured is for the unit.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.



Note

The **failover polltime interface** command applies to 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.

If a hello packet is not heard on the failover communication interface during the hold time, the standby unit switches to active and the peer is considered failed. Five missed consecutive *interface* hello packets cause interface testing.



Note

When CTIQBE traffic is passed through an FWSM 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 the Cisco CallManager are dropped, and the IP SoftPhone clients will need to reregister with the CallManager.

Examples

The following example sets the unit poll time frequency to 3 seconds:

```
hostname(config)# failover polltime 3
```

Related Commands

Command	Description
polltime interface	Specifies the interface polltime for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover preempt

To cause the primary unit in an Active/Standby failover configuration to become active on boot if the standby unit is currently in the active state, use the **failover preempt** command in global configuration mode. To remove the preemption, use the **no** form of this command.

failover preempt [*delay*]

no failover preempt [*delay*]

Syntax Description

delay The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds. If the *delay* is not specified, there is no delay.

Defaults

By default, there is no delay.

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
3.2(1)	This command was introduced.

Usage Guidelines

If the secondary unit in an Active/Standby pair is in the active state, the primary unit will automatically enter the standby state when it boots. It will remain in the standby state until a failover occurs or until you manually force it to the active state using the **no failover active** command on the secondary unit. Using the **failover preempt** command causes the primary unit to become active automatically and causes the secondary unit to enter the standby state.



Note

If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the peer unit.

Examples

The following example configures the primary unit to become active after a 5 second delay if it boots while the secondary unit is in the active state.

```
hostname(config)# failover
hostname(config)# failover lan unit primary
hostname(config)# failover preempt 5
hostname(config)# failover lan interface foverlink Vlan56
hostname(config)# failover replication http
```



```
hostname(config)# failover link foverlink Vlan56
hostname(config)# failover interface ip foverlink 10.1.1.1 255.255.255.0 standby 10.1.1.99
hostname(config)#
```

Related Commands

Command	Description
failover active	Forces a unit to become the active unit in an Active/Standby failover configuration.
failover lan unit	Specifies the unit as Primary or Secondary in an Active/Standby failover configuration.

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:

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

Release	Modification
3.1(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
```

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

By default, the FWSM 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 FWSM 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.
<i>group_id</i>	Failover group 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to allow the optional failover group ID.

Usage Guidelines

The **failover reset** command lets you 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 suspend-config-sync

To suspend failover configuration synchronization, use the **failover suspend-config-sync** command in global configuration mode. To disable failover, use the **no** form of this command.

failover suspend-config-sync

no failover suspend-config-sync

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
Global configuration	•	•	•	—	•

Release	Modification
2.3(1)	This command was introduced.

Command History

Usage Guidelines This command can be run only on the active unit. Running this command disables interface monitoring and logical updates.

Examples The following example suspends failover configuration synchronization:

```
hostname(config)# failover suspend-config-sync
hostname(config)#
```

Command	Description
clear configure failover	Removes the failover commands from the running configuration.
failover	Enables failover.
show running-config failover	Displays the failover commands in the running configuration.

Related Commands

filter activex

To remove ActiveX objects in HTTP traffic passing through the FWSM, use the **filter activex** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter activex {[*port*[-*port*] | **except** } *local_ip* *local_mask* *foreign_ip* *foreign_mask*]

no filter activex {[*port*[-*port*] | **except** } *local_ip* *local_mask* *foreign_ip* *foreign_mask*]

Syntax Description

except	Creates an exception to a previous filter condition.
<i>foreign_ip</i>	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.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>port</i>	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 the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide</i> .
<i>port-port</i>	(Optional) Specifies a port range.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

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 **filteractivex** 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 FWSM cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command.

Examples

The following example specifies that Activex objects are blocked on all outbound connections:

```
hostname(config)# filteractivex 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 FWSM.
show running-config filter	Displays filtering configuration.
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 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* *local_mask* *foreign_ip* *foreign_mask*] [**allow**]
[**interact-block**]

no filter ftp {[*port*[-*port*] | **except** } *local_ip* *local_mask* *foreign_ip* *foreign_mask*] [**allow**]
[**interact-block**]

Syntax Description

<i>port</i>	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.
<i>port-port</i>	(Optional) Specifies a port range.
except	Creates an exception to a previous filter condition.
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>foreign_ip</i>	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.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . 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 FWSM without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the FWSM 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The **filter ftp** command lets you identify the FTP traffic to be filtered by a Websense server. FTP filtering is not supported on N2H2 servers.

After enabling this feature, when a user issues an FTP GET request to a server, the FWSM sends the request to the FTP server and to the Websense server at the same time. If the Websense server permits the connection, the FWSM 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 server denies the connection, the FWSM alters the FTP return code to show that the connection was denied. For example, the FWSM 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 server.
filter java	Removes Java applets from HTTP traffic passing through the FWSM.
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 https

To identify the HTTPS traffic to be filtered by a 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 local_mask foreign_ip foreign_mask*] [**allow**]

no filter https {[*port*[-*port*] | **except**] *local_ip local_mask foreign_ip foreign_mask*] [**allow**]

Syntax Description

<i>port</i>	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.
<i>port-port</i>	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous filter condition.
<i>dest-port</i>	The destination port number.
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>foreign_ip</i>	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.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . 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 FWSM without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the FWSM 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The FWSM supports filtering of HTTPS and FTP sites using an external Websense filtering server.

**Note**

HTTPS is not supported for the 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 FWSM 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
filteractivex	Removes ActiveX objects from HTTP traffic passing through the FWSM.
filterjava	Removes Java applets from HTTP traffic passing through the FWSM.
filterurl	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 java

To remove Java applets from HTTP traffic passing through the FWSM, 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

<i>port</i>	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.
<i>port-port</i>	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous filter condition.
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>foreign_ip</i>	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.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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.

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 FWSM cannot block the tag. If Java applets are known to be in <object> tags, use the **filteractivex** 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
filteractivex	Removes ActiveX objects from HTTP traffic passing through the FWSM.
filterurl	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 local_mask foreign_ip foreign_mask [allow]
[cgi-truncate] [longurl-truncate | longurl-deny] [proxy-block]
```

```
no filter url {[port[-port] | except } local_ip local_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 FWSM without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the FWSM 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.
<i>foreign_ip</i>	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.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . 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.)
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . 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 Websense server if the URL is over the URL buffer limit.
<i>mask</i>	Any mask.
[<i>port</i> [- <i>port</i>]]	(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 FWSM.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM without filtering. Used without the **allow** option and with the server off line, the FWSM 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 FWSM now passes control to an alternate server if the N2H2 or Websense server goes off line.

The N2H2 or Websense server works with the FWSM to deny users from access to websites based on the company security policy.

Using the Websense Filtering Server

Websense protocol Version 4 enables group and username authentication between a host and a FWSM. The FWSM performs a username lookup, and then the 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 FWSM 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 FWSM to use the user authentication table to map the host IP address to the username.

Information on Websense is available at the following website:

<http://www.websense.com/>

Configuration Procedure

To filter URLs, perform the following steps:

-
- 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.
-



Note The **url-cache** command does not update Websense logs, which may affect Websense accounting reports. Accumulate Websense run logs before using the **url-cache** command.

- Step 4** To view run information, use the **show url-cache statistics** and the **show perfmon** commands.
-

Working with Long URLs

Filtering URLs up to 4 KB is supported for the Websense filtering server, and up to 1159 bytes 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 FWSM drops the packet.

The **longurl-truncate** option causes the FWSM 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 FWSM performance.

Buffering HTTP Responses

By default, when a user issues a request to connect to a specific website, the FWSM 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-limit* with the maximum number of blocks that will be buffered. The permitted values are from 0 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
filteractivex	Removes ActiveX objects from HTTP traffic passing through the FWSM.
filterjava	Removes Java applets from HTTP traffic passing through the FWSM.
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.

firewall autostate (IOS)

To enable autostate messaging, use the **firewall autostate** command in global configuration mode. To disable autostate, use the **no** form of this command. Autostate messaging lets the FWSM quickly detect that a switch interface has failed or has come up.

firewall autostate

no firewall autostate

Syntax Description This command has no arguments or keywords.

Defaults By default, autostate is disabled.

Command Modes Global configuration.

Command History	Release	Modification
	12.2(18)SXF5	This command was introduced.

Usage Guidelines Using Catalyst operating system software Release 8.4(1) and higher or Cisco IOS software Release 12.2(18)SXF5 and higher, the supervisor engine can send autostate messages to the FWSM about the status of physical interfaces associated with FWSM VLANs. For example, when all physical interfaces associated with a VLAN go down, the autostate message tells the FWSM that the VLAN is down. This information lets the FWSM declare the VLAN as down, bypassing the interface monitoring tests normally required for determining which side suffered a link failure. Autostate messaging provides a dramatic improvement in the time the FWSM takes to detect a link failure (a few milliseconds as compared to up to 45 seconds without autostate support).

The switch supervisor sends an autostate message to the FWSM when:

- The last interface belonging to a VLAN goes down.
- The first interface belonging to a VLAN comes up.



Note

The Catalyst operating system software has autostate messaging enabled by default, and it is not configurable.

Examples The following example enables autostate:

```
Router(config)# firewall autostate
```

Related Commands

Command	Description
show firewall autostate	Shows the setting of the autostate feature.

firewall module (IOS)

To assign firewall groups to the FWSM, enter the **firewall module** command in global configuration mode. To remove the groups, use the **no** form of this command.

```

firewall module module_number vlan-group firewall_group

no firewall module module_number vlan-group firewall_group
    
```

Syntax Description	<i>module_number</i>	Specifies the module number. Use the show module command to view installed modules and their numbers.
	vlan-group <i>firewall_group</i>	Specifies one or more group numbers as defined by the firewall vlan-group command: - A single number (<i>n</i>) - A range (<i>n-x</i>) Separate numbers or ranges by commas. For example, enter the following numbers: 5,7-10

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines

In Cisco IOS software, create up to 16 firewall VLAN groups (using the **firewall vlan-group** command), and then assign the groups to the FWSM using the **firewall module** command.. For example, you can assign all the VLANs to one group, or you can create an inside group and an outside group, or you can create a group for each customer. Each group can contain unlimited VLANs.

You cannot assign the same VLAN to multiple firewall groups; however, you can assign multiple firewall groups to an FWSM and you can assign a single firewall group to multiple FWSMs. VLANs that you want to assign to multiple FWSMs, for example, can reside in a separate group from VLANs that are unique to each FWSM.

Examples

The following example shows how you can create three firewall VLAN groups: one for each FWSM, and one that includes VLANs assigned to both FWSMs.

```

Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
    
```

```
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
-----
50 55-57
51 70-85
52 100
```

The following is sample output from the **show firewall module** command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
5      50,52
8      51,52
```

Related Commands

Command	Description
firewall vlan-group	Assigns VLANs to a VLAN group.
show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

firewall multiple-vlan-interfaces (IOS)

To allow you to add more than one SVI to the FWSM, use the **firewall multiple-vlan-interfaces** command in global configuration mode. To disable this feature, use the **no** form of this command.

- firewall multiple-vlan-interfaces**
- no firewall multiple-vlan-interfaces**

Syntax Description	This command has no arguments or keywords.	
Defaults	By default, multiple SVIs are not allowed.	
Command Modes	Global configuration.	
Command History	Release	Modification
	Preexisting	This command was preexisting.
Usage Guidelines	A VLAN defined on the MSFC is called a switched virtual interface. If you assign the VLAN used for the SVI to the FWSM, then the MSFC routes between the FWSM and other Layer 3 VLANs. For security reasons, by default, only one SVI can exist between the MSFC and the FWSM. For example, if you misconfigure the system with multiple SVIs, you could accidentally allow traffic to pass around the FWSM by assigning both the inside and outside VLANs to the MSFC. However, you might need to bypass the FWSM in some network scenarios. For example, if you have an IPX host on the same Ethernet segment as IP hosts, you will need multiple SVIs. Because the FWSM in routed firewall mode only handles IP traffic and drops other protocol traffic like IPX (transparent firewall mode can optionally allow non-IP traffic), you might want to bypass the FWSM for IPX traffic. Make sure to configure the MSFC with an access list that allows only IPX traffic to pass on the VLAN. For transparent firewalls in multiple context mode, you need to use multiple SVIs because each context requires a unique VLAN on its outside interface. You might also choose to use multiple SVIs in routed mode so you do not have to share a single VLAN for the outside interface.	

Examples

The following example shows a typical configuration with multiple SVIs:

```

Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end

```


Router#

The following is sample output from the **show interface** command:

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 55.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  4 packets output, 256 bytes, 0 underruns
  0 output errors, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to the FWSM.
firewall vlan-group	Defines a VLAN group.

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. You can set the mode independently for each security context in multiple context mode.

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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	You can set the mode independently for each security context in multiple context mode. Previously, you entered this command in the system execution space, and set the mode for all contexts.

Usage Guidelines When you change modes, the FWSM 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 FWSM that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the FWSM 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 FWSM 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.

firewall vlan-group (IOS)

To assign VLANs to a firewall group, enter the **firewall vlan-group** command in global configuration mode. To remove the VLANs, use the **no** form of this command.

```

firewall vlan-group firewall_group vlan_range

no firewall vlan-group firewall_group vlan_range
    
```

Syntax Description		
<i>firewall_group</i>		Specifies the group ID as an integer.
<i>vlan_range</i>		Specifies the VLANs assigned to the group. The <i>vlan_range</i> can be one or more VLANs (2 to 1000 and from 1025 to 4094) identified in one of the following ways: - A single number (<i>n</i>) - A range (<i>n-x</i>) Separate numbers or ranges by commas. For example, enter the following numbers: 5,7-10,13,45-100
	Note	Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.

Defaults

No default behavior or values.

Command Modes

Global configuration.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines

In Cisco IOS software, create up to 16 firewall VLAN groups using the **firewall vlan-group** command, and then assign the groups to the FWSM (using the **firewall module** command). For example, you can assign all the VLANs to one group, or you can create an inside group and an outside group, or you can create a group for each customer. Each group can contain unlimited VLANs.

You cannot assign the same VLAN to multiple firewall groups; however, you can assign multiple firewall groups to an FWSM and you can assign a single firewall group to multiple FWSMs. VLANs that you want to assign to multiple FWSMs, for example, can reside in a separate group from VLANs that are unique to each FWSM.

Examples

The following example shows how you can create three firewall VLAN groups: one for each FWSM, and one that includes VLANs assigned to both FWSMs.

```
Router(config)# firewall vlan-group 50 55-57
```

```
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
-----
50 55-57
51 70-85
52 100
```

The following is sample output from the **show firewall module** command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
5      50,52
8      51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an FWSM.
show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

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 {flash:}

Syntax Description

flash: Specifies the internal Flash memory, followed by a colon.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1(1)	Support for 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.

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.

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*

no fqdn

Syntax Description

fqdn Specifies the fully qualified domain name. The maximum length of *fqdn* is 64 characters.

Defaults

The default setting is not to include the FQDN.

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 configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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(ca-trustpoint)# fqdn engineering
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 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 restore the value to the default, use the **no** form of the command.

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

Syntax Description

chain <i>limit</i>	Specifies the maximum number of packets into which a full IP packet can be fragmented, between 1 and 8200. The default is 24.
<i>interface</i>	(Optional) Specifies the FWSM interface. If an interface is not specified, the command applies to all interfaces.
size <i>limit</i>	Sets the maximum number of packets that can be in the IP reassembly database waiting for reassembly, between 1 and 30000. The default is 200.
timeout <i>limit</i>	Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive, between 1 and 30. The default is 5. 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:

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

Command History

Release	Modification
1.1(3)	This command was introduced.
3.1(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 FWSM accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the FWSM to prevent fragmented packets from traversing the FWSM 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 FWSM 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.

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.

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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive. The FWSM 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 FWSM 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.

ftp-map

To identify a specific map for defining the parameters for strict FTP inspection, use the **ftp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

ftp-map *map_name*

no ftp-map *map_name*

Syntax Description

map_name The name of the FTP map.

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
3.1(1)	This command was introduced.

Usage Guidelines

Use the **ftp-map** command to identify a specific map to use for defining the parameters for strict FTP inspection. When you enter this command, the system enters the FTP map configuration mode, which lets you enter the different commands used for defining the specific map. Use the **request-command deny** command to prevent the FTP client from sending specific commands to the FTP server.

After defining the FTP map, use the **inspect ftp strict** command to enable the map. Then 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 FTP traffic, define an FTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
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 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-command deny	Specifies FTP commands to disallow.



CHAPTER

13

gateway through http-map 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
<i>ip_address</i>	The IP address of the gateway.
<i>group_id</i>	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:

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

Command History

Release	Modification
3.1(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.
<i>mapped_ifc</i>	Specifies the name of the interface connected to the mapped IP address network.
<i>mapped_ip</i> [- <i>mapped_ip</i>]	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).
<i>nat_id</i>	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 <i>mask</i>	(Optional) Specifies the network mask for the <i>mapped_ip</i> . This mask does not specify a network when paired with the <i>mapped_ip</i> ; rather, it specifies the subnet mask assigned to the <i>mapped_ip</i> when it is assigned to a host. If you want to configure a range of addresses, you need to specify <i>mapped_ip-mapped_ip</i> . 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2.(1)	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-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

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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
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. 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 FWSM prevents the user from connecting. If you do not configure group-lock, the FWSM authenticates users without regard to the assigned group.

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 <i>tunnel-grp-name</i>	Specifies the name of an existing tunnel group that the FWSM 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:

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

Command History

Release	Modification
3.1(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

<i>obj_grp_id</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Protocol, network, service, icmp-type configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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 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 <i>server_group</i>	Specifies the group policy as external and identifies the AAA server group for the FWSM to query for attributes.
from <i>group-policy_name</i>	Initializes the attributes of this internal group policy to the values of a pre-existing group policy.
internal	Identifies the group policy as internal.
<i>name</i>	Specifies the name of the group policy.
password <i>server_password</i>	Provides the password to use when retrieving attributes from the external AAA server group.

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
3.1(1)	This command was introduced.

Usage Guidelines

A default group policy, named “DefaultGroupPolicy,” always exists on the FWSM. However, this default group policy does not take effect unless you configure the FWSM to use it. For configuration instructions, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

The DefaultGroupPolicy has these AVPs:

Attribute	Default Value
wins-server	none
dns-server	none

Attribute	Default Value
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	IPSec 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	10000
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled

Examples

The following example shows how to create an internal group policy with the name “FirstGroup”:

```
hostname(config)# group-policy FirstGroup internal
```

The following 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 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.

group-policy attributes

To enter the group-policy attributes mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. The attributes mode lets you configure AVPs for a specified group policy.

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:

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

Command History

Release	Modification
3.1(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.

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
<code>clear configure group-policy</code>	Removes the configuration for a particular group policy or for all group policies.
<code>group-policy</code>	Creates, edits, or removes a group policy.
<code>show running-config group-policy</code>	Displays the running configuration for a particular group policy or for all group policies.

gtp-map

To identify a specific map to use for defining the parameters for GTP, use the **gtp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

gtp-map *map_name*

no gtp-map *map_name*



Note

GTP inspection requires a special license. If you enter the **gtp-map** command on a FWSM without the required license, the FWSM displays an error message.

Syntax Description

<i>map_name</i>	The name of the GTP map.

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
3.1(1)	This command was introduced.

Usage Guidelines

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 and how the FWSM ensures secure access over wireless networks, refer to the “Applying Application Layer Protocol Inspection” chapter in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

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. 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.

Table 13-1 GTP Map Configuration Commands

Command	Description
description	Specifies the GTP configuration map description.
drop	Specifies the message ID, APN, or GTP version to drop.
mcc	Specifies the three-digit Mobile Country Code (000 - 999). One or two- digit entries will be prepended with 0s
message-length	Specifies the message length min and max.
permit errors	Permits packets with errors or different GTP versions.
request-queue	Specifies the maximum requests allowed in the queue.
timeout (gtp-map)	Specifies the idle timeout for the GSN, PDP context, requests, signaling connections, and tunnels.
tunnel-limit	Specifies the maximum number of tunnels allowed.

Examples

The following example shows how to use the **gtp-map** command to identify a specific map (gtp-policy) to use for defining the parameters for GTP:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)#
```

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-cmap)# match access-list gtp-acl
hostname(config-cmap)# exit
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# request-queue 300
hostname(config-gtpmap)# permit mcc 111 mnc 222
hostname(config-gtpmap)# message-length min 20 max 300
hostname(config-gtpmap)# drop message 20
hostname(config-gtpmap)# tunnel-limit 10000
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 outside
```

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.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

h225-map

To define an H.225 application inspection map, use the **h225-map** command in global configuration mode. To remove the map, use the **no** form of this command.

h225-map *map_name*

no h225-map *map_name*

Syntax Description

map_name The name of the H.225 map.

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
FWSM 3.1	This command was introduced.

Usage Guidelines

An H.225 map allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling.

. The H.225 map provides information about the HSI and its associated endpoints, which is required to establish this connection without compromising the security of the network protected by the FWSM.

When you enter the **h225-map** command, the system enters the H.225 map configuration mode, which lets you enter the different commands used for defining the specific map.

One H.225 map can contain a maximum of five HSI groups. Each HSI group can contain a maximum of ten endpoints.

Examples

The following example shows how to define an H.225 map.

```
hostname(config)# h225-map sample_map
hostname(config-h225-map)# hsi-group 1
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
hostname(config-h225-map-hsi-grp)# exit
```


Related Commands	Commands	Description
	endpoint	Defines the endpoint associated with an HSI group.
	hsi	Defines the HSI associated with an HSI group.
	hsi-group	Defines an HSI group and enables HSI group configuration mode.
	inspect h323 h225	Applies an H.225 map to H.323 application inspection.

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

<i>as-number</i>	The autonomous system number of the EIGRP routing process.
<i>seconds</i>	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:

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

Command History

Release	Modification
4.0(1)	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

<i>command</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

hold-time

To specify the hold time advertised by the FWSM 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

<i>as-number</i>	The autonomous system number of the EIGRP routing process.
<i>seconds</i>	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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the FWSM. The EIGRP neighbors on that interface use this value to determine the availability of the FWSM. If they do not receive a hello packet from the FWSM during the advertised hold time, the EIGRP neighbors will consider the FWSM 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 FWSM 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
```

hold-time

Related Commands

Command	Description
hello-interval	Specifies the interval between EIGRP hello packets sent on an interface.

hostname

To set the FWSM 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

<i>name</i>	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 is FWSM.

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
1.1(1)	This command was introduced.

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 associate an HSI with an HSI group, use the **hsi** command in HSI group configuration mode. To remove the HSI, use the **no** form of this command.

hsi *ip address*

no hsi *ip address*

Syntax Description

ip address The IP address of the HSI.

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
HSI group configuration	•	•	•	•	—

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

An HSI group allows the FWSM to open dynamic, port-specific pinholes for enabling H.323 connections when a Cisco CallManager tries to establish a connection between H.323 endpoints.

Up to five HSI groups can be associated with a single H.225 map. Each HSI group can contain a maximum of ten endpoints.

Examples

The following example shows how to define an H.225 map.

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
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
hostname(config-h225-map-hsi-grp)# exit
```

Related Commands

Commands	Description
endpoint	Defines the endpoint associated with an HSI group.
hsi-group	Defines an HSI group and enables HSI group configuration mode.

Commands	Description
h225-map	Defines an H.225 map and enables H.225 map configuration mode.
inspect h323 h225	Applies an H.225 map to H.323 application inspection.

hsi-group

To define an HSI group, use the **hsi-group** command in H.225 map configuration mode. To remove the HSI group, use the **no** form of this command.

hsi-group *group_ID*

no hsi-group *group_ID*

Syntax Description

<i>group_name</i>	A number, from 0 to 2147483647, that identifies the HSI group.

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
H.225 map configuration	•	•	•	•	—

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

When you enter the **hsi-group** command, the system enters the HSI group configuration mode, which lets you enter the different commands used for defining the specific map.

A HSI group allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling.

Up to five HSI groups can be associated with a single H.225 map. Each HSI group can contain a maximum of ten endpoints. You must configure an HSI within the group before configuring any endpoints. You must remove all endpoints and the HSI before removing the HSI group.

Examples

The following example shows how to define an H.225 map.

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
hostname(config-h225-map-hsi-grp)# hsi 192.168.100.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.102
hostname(config-h225-map-hsi-grp)# exit
hostname(config-h225-map)# hsi-group 2
hostname(config-h225-map-hsi-grp)# hsi 192.168.200.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.102
```

```
hostname(config-h225-map-hsi-grp) # exit
```

Related Commands

Commands	Description
endpoint	Defines the endpoint associated with an HSI group.
hsi	Defines the HSI associated with an HSI group.
h225-map	Defines an H.225 map and enables H.225 map configuration mode.
inspect h323 h225	Applies an H.225 map to H.323 application inspection.

http

To specify hosts that can access the HTTP server internal to the FWSM, 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

<i>interface_name</i>	Provides the name of the FWSM interface through which the host can access the HTTP server.
<i>ip_address</i>	Provides the IP address of a host that can access the HTTP server.
<i>subnet_mask</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM.

Command	Description
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 authentication-certificate

To require authentication via certificate from users who are establishing HTTPS connections, use the **http authentication-certificate** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command. To remove all **http authentication-certificate** commands from the configuration, use the **no** version without arguments.

The FWSM validates certificates against the PKI trust points. If a certificate does not pass validation, the FWSM closes the SSL connection.

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

Syntax Description

interface Specifies the interface on the FWSM that requires certificate authentication.

Defaults

HTTP certificate authentication is disabled.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

You can configure certificate authentication for each interface, such that connections on a trusted/inside interface do not have to provide a certificate. You can use the command multiple times to enable certificate authentication on multiple interfaces.

Validation occurs before the URL is known, so this affects both WebVPN and ASDM access.

The ASDM uses its own authentication method in addition to this value. That is, it requires both certificate and username/password authentication if both are configured, or just username/password if certificate authentication is disabled.

Examples

The following example shows how to require certificate authentication for clients connecting to the interfaces named outside and external:

```
hostname(config)# http authentication-certificate inside
hostname(config)# http authentication-certificate external
```

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 FWSM interface through which the host accesses the HTTP server.
	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 FWSM HTTPS server for ASDM, use the **http server enable** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command.

http server enable

no http server enable

Defaults

The HTTP server is disabled.

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
1.1(1)	This command was introduced.

Examples

The following example shows how to enable the HTTPS 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 HTTPS server.
http	Specifies hosts that can access the HTTPS server by IP address and subnet mask. Specifies the FWSM interface through which the host accesses the HTTPS server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the FWSM.
show running-config http	Displays the hosts that can access the HTTPS server, and whether or not the HTTPS server is enabled.

http-map

To create an HTTP map for applying enhanced HTTP inspection parameters, use the **http-map** command in global configuration mode. To remove the command, use the **no** form of this command.

http-map *map_name*

no http-map *map_name*

Syntax Description

map_name The name of the HTTP map.

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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The enhanced HTTP inspection feature, which is also known as an application firewall, verifies that HTTP messages conform to RFC 2616, use RFC-defined and supported extension methods, and comply with various other criteria. This can help prevent attackers from using HTTP messages for circumventing network security policy.



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.

In many cases, you can configure the criteria and how the FWSM responds when the criteria are not met. The criteria that you can apply to HTTP messages include the following:

- Does not include any method on a configurable list.
- 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.

Table 13-2 summarizes the configuration commands available in HTTP map configuration mode. For detailed syntax for a command, see the corresponding command entry in this guide.

Table 13-2 HTTP Map Configuration Commands

Command	Description
content-length	Enables inspection based on the length of the HTTP content.
content-type-verification	Enables inspection based on the type of HTTP content.
max-header-length	Enables inspection based on the length of the HTTP header.
max-uri-length	Enables inspection based on the length of the URI.
port-misuse	Enables port misuse application inspection.
request-method	Enables inspection based on the HTTP request method.
strict-http	Enables strict HTTP inspection.
transfer-encoding	Enables inspection based on the transfer encoding type.

Examples

The following is sample output showing 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 FWSM 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.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.



CHAPTER

14

icmp through im Commands

icmp

To configure access rules for ICMP traffic that terminates at a FWSM 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.
<i>icmp_type</i>	(Optional) ICMP message type (see Table 3).
<i>if_name</i>	The interface name.
<i>ip_address</i>	The IP address of the host sending ICMP messages to the interface.
<i>net_mask</i>	The mask to be applied to <i>ip_address</i> .
permit	Permit access if the conditions are matched.

Defaults

The default behavior of the FWSM is to allow all ICMP traffic *to* the FWSM interfaces. However, by default the FWSM does not respond to ICMP echo requests directed to a broadcast address. The FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any FWSM interface. If no ICMP control list is configured, then the FWSM accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 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
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

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-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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
3.1(1)	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 FWSM 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.

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.

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

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-subif)# no igmp
```

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the FWSM and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

Related Commands

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 an 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command configures a FWSM interface to be a member of a multicast group. The **igmp join-group** command causes the FWSM 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 Vlan101
hostname(config-subif)# igmp join-group 255.2.2.2
```

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

<i>number</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced. It replaced the igmp max-groups command.

Examples

The following example limits the number of hosts that can join on the interface to 250:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 Vlan101  
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 Vlan101
hostname(config-subif)# 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

<i>seconds</i>	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:

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

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When configured with the **igmp static-group** command, the FWSM interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the FWSM both accept and forward multicast packets for a specific 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 Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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 Vlan101
hostname(config-subif)# 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 lsa mospf

To suppress the sending of syslog messages when the router receives link-state advertisement (LSA) Type 6 Multicast OSPF (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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

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:

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

Command History

Release	Modification
4.0(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.



CHAPTER

15

inspect ctique 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM.

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 FWSM, 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 FWSM, 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, use 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 FWSM. 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 dcerpc [*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:

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

Command History

Release	Modification
3.2(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)# 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), use the **inspect dns** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. Use the **inspect dns** command to specify the maximum DNS packet length. To disable DNS inspection, use the **no** form of this command.

inspect dns [**maximum-length** *max_pkt_length*]

no inspect dns [**maximum-length** *max_pkt_length*]

Syntax Description

maximum-length	(Optional) Specifies the maximum DNS packet length. The default is 512. If you enter the inspect dns command without the maximum-length option, DNS packet size is not checked.
<i>max_pkt_length</i>	The maximum DNS packet length. Longer packets will be dropped.

Defaults

This command is enabled by default.

The default **maximum-length** for the DNS packet size is 512.

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
3.1(1)	This command was introduced, replacing the fixup protocol dns command, which is now deprecated.

Usage Guidelines

DNS guard tears down the DNS session associated with a DNS query as soon as the DNS reply is forwarded by the FWSM. 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 FWSM 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.

**Note**

If you enter the **inspect dns** command without the **maximum-length** option, DNS packet size is not checked

- 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 FWSM 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 changes the maximum DNS packet length to 1500 bytes. Although DNS inspection is enabled by default, you still need to create a traffic map to identify DNS traffic and then apply the policy map to the appropriate interface.

```
hostname(config)# class-map dns-port
hostname(config-cmap)# match port udp eq 53
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
```

```
hostname(config-pmap-c)# inspect dns maximum-length 1500
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

To change the maximum DNS packet length for all interfaces, use the **global** parameter in place of **interface outside**.

The following example shows how to disable DNS:

```
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class dns-port
hostname(config-pmap-c)# no inspect dns
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

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 extended SMTP application inspection, 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

no inspect esmtp

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the FWSM and by adding monitoring capabilities.

Extended SMTP application inspection, as enabled by the **inspect esmtp** command, occurs in control plane path processing; therefore, it occurs on the single, general purpose processor on the FWSM.

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 provided by the **inspect 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 FWSM supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions 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.

**Note**

If a policy map contains both the **inspect smtp** command and the **inspect esmtp** command, only the first command listed in the policy map is applied to matching traffic.

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 may hang 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>).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character | is deleted (changed to a blank space) and | are only allowed if they are used to define a mail address | must be preceded by “<”).
- Unexpected transition by the SMTP server.
- For unknown commands, the FWSM 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 smtp	Enables debug information for SMTP.
inspect smtp	Enables standard (non-extended) SMTP application inspection.
policy-map	Associates a class map with specific security actions.
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	<i>map_name</i>	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 FWSM listens to port 21 for FTP 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
	3.1(1)	This command was introduced, replacing the fixup protocol ftp command, which is now deprecated.

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

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**

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.

**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 FWSM 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 FWSM, 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

The following example identifies FTP traffic, defines an FTP map, defines a policy, enables strict FTP inspection, and applies the policy to the outside interface:

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-inbound_ftp)# request-command deny put stou appe
hostname(config-ftp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

To enable strict FTP application inspection for all interfaces, use the **global** parameter in place of **interface outside**.



Note

Only specify the port for the FTP control connection and not the data connection. The FWSM stateful inspection engine dynamically prepares the data connection as necessary.

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 FWSM without the required license, the FWSM 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:

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

Command History

Release	Modification
3.1(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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

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 **allow**, **reset**, or **drop**. 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 string **gtp**, used as a port value, is automatically converted to the port value 3386. 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, use 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	Clears global GTP statistics.
inspect gtp	Displays detailed information about GTP inspection.
service-policy	Applies a policy map to one or more interfaces.

inspect h323

To enable H.323 application inspection or to change the ports to which the FWSM 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 [h225_map] | ras}
```

```
no inspect h323 {h225 [h225_map] | ras}
```

Syntax Description

h225	Enables H.225 signalling inspection.
<i>h225_map</i>	(Optional) The name of an H.225 application inspection map, which defines the configuration required to use the FWSM in topologies involving Cisco HSI and H.323 endpoints'.
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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol h323 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 FWSM 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 FWSM 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 FWSM.

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 FWSM 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 FWSM 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 FWSM, 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 FWSM opens an H.225 connection based on inspection of the ACF message. If the FWSM 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 FWSM 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 FWSM 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 TPMT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPMT header does not necessarily need to be sent in the same TCP packet as the H.225/H.245 message, the FWSM must remember the TPMT length to process/decode the messages properly. The FWSM keeps a data structure for each connection and that data structure contains the TPMT length for the next expected message.

If the FWSM needs to NAT any IP addresses, then it will have to change the checksum, the UIIE (user-user information element) length, and the TPMT, if included in the TCP packet with the H.225 message. If the TPMT is sent in a separate TCP packet, then the FWSM will proxy ACK that TPMT and append a new TPMT to the H.245 message with the new length.

**Note**

The FWSM 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.
- 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 FWSM.
- 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, use other static routing or dynamic routing.

Using an H.225 Map

An H.225 map allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling. The H.225 map provides information about the HSI and its associated endpoints, which is required to establish this connection without compromising the security of the network protected by the FWSM.

Table 15-1 summarizes the commands used to perform the required configuration:

Table 15-1 H..225 Configuration Commands

Command	Configuration mode	Description
h225-map	Global configuration mode	Defines an H.225 application inspection map and enables H.225 map configuration mode. One H225 map can contain a maximum of five HSI groups.
hsi-group	H.225 map configuration mode	Defines an HSI group and enables HSI group configuration mode. Each HSI group can contain a maximum of ten endpoints
hsi	HSI group configuration mode	Identifies the HSI.
endpoint	HSI group configuration mode	Identifies one or more endpoints within the HSI group.

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 inspection for all interfaces, enter the **global** parameter in place of **interface outside**

The following example illustrates the H.225 configuration required when an FWSM interconnects H.323 endpoints and a Cisco CallManager must establish a connection between these endpoints:

```
hostname(config)# access-list h323_acl permit udp any any eq 1720
hostname(config)# access-list h323_acl permit udp any any eq 1721
hostname(config)# class-map h323-traffic
hostname(config-cmap)# match access-list h323_acl
hostname(config-cmap)# exit
hostname(config)# h225-map sample_map
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
hostname(config-h225-map-hsi-grp)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class h323_port
hostname(config-pmap-c)# inspect h323 ras
hostname(config-pmap-c)# inspect h323 h225 sample_map
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy 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 FWSM.
show h245	Displays information for H.245 sessions established across the FWSM by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
timeout	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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol http 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 FWSM 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. To remove the configuration, use the **no** form of this command.

- 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol icmp 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 FWSM 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 FWSM 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. To remove the configuration, use the **no** form of this command.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol icmp error 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 FWSM overwrites the packet with the translated IP addresses.

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 FWSM 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 or to change the ports to which the FWSM listens, 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol ils 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.

Use the *port* option to change the default port assignment from 389. Use the *-port* option to apply ILS inspection to a range of port numbers.

The FWSM 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 FWSM 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 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 H.225 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 mgcp

To enable MGCP application inspection or to change the ports to which the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol mgcp 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 FWSM 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.

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 FWSM.
	timeout	Sets the maximum idle time duration for different protocols and session types.

inspect netbios

To enable NetBIOS application inspection or to change the ports to which the FWSM 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

no inspect netbios

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:

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

The **inspect netbios** command enables or disables application inspection for the NetBIOS protocol.

Examples

You enable the NetBIOS inspection engine as shown in the following example, which creates a class map to match NetBIOS traffic on the default UDP ports (137 and 138). The service policy is then applied to the outside interface.

```
hostname(config)# class-map netbios-port
hostname(config-cmap)# match port udp range 137 138
hostname(config-cmap)# exit
hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class netbios-port
hostname(config-pmap-c)# inspect netbios
hostname(config-pmap-c)# exit
hostname(config)# service-policy netbios_policy interface outside
```

To enable NetBIOS 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 pptp

To enable PPTP application inspection or to change the ports to which the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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 dynamically 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. I

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 rsh

To enable RSH application inspection or to change the ports to which the FWSM 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 disabled 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
3.1(1)	This command was introduced, replacing the fixup protocol rsh 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 FWSM 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

no inspect rtsp

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol rtsp command, which is now deprecated.

Usage Guidelines

The **inspect rtsp** command lets the FWSM 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 FWSM 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 FWSM parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the FWSM and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the FWSM 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 FWSM 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

To use RealPlayer, it is important to properly configure transport mode. For the FWSM, 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 FWSM, 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 FWSM, add an **inspect rtsp port** command statement.

Restrictions and Limitations

The following restrictions apply to the **inspect rtsp** command:

- The FWSM does not support multicast RTSP or RTSP messages over UDP.
- PAT is not supported with the **inspect rtsp** command.
- The FWSM does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The FWSM cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and the FWSM cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of NATs the FWSM 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 FWSM 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 [*map_name*]

no inspect sip [*map_name*]

Syntax Description

map_name (Optional) The name of a SIP map created using the **sip-map** command. A SIP map lets you specify additional inspection parameters for SIP inspection, such as IP address privacy, which you can configure with the **ip-address-privacy** command in SIP map configuration mode.

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		
	Routed	Transparent	Single	Multiple Context	System
Class configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol sip 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 FWSM 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 FWSM, 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 FWSM, 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 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 FWSM, unless the FWSM 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, use 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)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# service-policy sip_policy interface outside
hostname(config)#
```

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.
policy-map	Associates a class map with specific security actions.
show sip	Displays information about SIP sessions established through the FWSM.
show conn	Displays the connection state for different connection types.
sip-map	Defines additional SIP inspection parameters.

inspect skinny

To enable SCCP (Skinny) application inspection or to change the ports to which the FWSM 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

no inspect skinny

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol skinny 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 FWSM recognize SCCP Version 3.3. The functionality of the application layer software ensures that all SCCP signaling and media packets can traverse the FWSM 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 FWSM supports all versions through Version 3.3.2. The FWSM 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 FWSM also supports DHCP options 150 and 66, which allow the FWSM 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 FWSM currently does not support NAT or PAT for the file content transferred via TFTP. Although the FWSM does support NAT of TFTP messages, and opens a pinhole for the TFTP file to traverse the FWSM, the FWSM cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone 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, use 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 FWSM.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect smtp

To enable non-extended SMTP application inspection, use the **inspect smtp** 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 smtp

no inspect smtp

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol smtp command, which is now deprecated.

Usage Guidelines

SMTP application inspection provides basic protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the FWSM and by adding monitoring capabilities. The application inspection process for SMTP does not include for extended SMTP sessions.

SMTP application inspection, as enabled by the **inspect smtp** command, occurs in fast path processing; therefore, it occurs on one of the three network processors on the FWSM.

The **inspect smtp** command includes the functionality previously provided by the **fixup smtp** command. It supports seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET). Other SMTP and extended SMTP commands 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.



Note

If a policy map contains both the **inspect smtp** command and the **inspect esmtp** command, only the first command listed in the policy map is applied to matching traffic.

The **inspect smtp** 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 may hang 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.
- 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>).
- The MAIL and RCPT commands specify who are the sender and the receiver of the mail. Mail addresses are scanned for strange characters. The pipeline character | is deleted (changed to a blank space) and | are only allowed if they are used to define a mail address | must be preceded by "<").
- Unexpected transition by the SMTP server.
- For unknown commands, the FWSM 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 smtp
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 smtp	Enables debug information for SMTP.
inspect esmtp	Enables extended SMTP application inspection.
policy-map	Associates a class map with specific security actions.
show conn	Displays the connection state for different connection types, including SMTP.

inspect snmp

To enable SNMP application inspection or to change the ports to which the FWSM 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:

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

Command History

Release	Modification
3.1(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the fixup protocol sqlnet command, which is now deprecated.

Usage Guidelines

The SQL*Net protocol consists of different packet types that the FWSM handles to make the data stream appear consistent to the Oracle applications on either side of the FWSM.

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.

The FWSM 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 FWSM, 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 FWSM 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 disabled 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
3.1(1)	This command was introduced, replacing the fixup protocol rpc command, which is now deprecated.

Usage Guidelines

To enable Sun RPC application inspection or to change the ports to which the FWSM 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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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:

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

Command History

Release	Modification
3.2(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 FWSM 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 disabled 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
3.1(1)	This command was introduced.

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 FWSM must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the FWSM. 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 FWSM 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

interface through issuer-name Commands

interface

To add an interface to the configuration and enter interface configuration mode, use the **interface** command in global configuration mode.

interface {*vlan <n>* | *mapped_name*}

Syntax Description

<i>vlan <n></i>	In multiple context mode, lets you configure the name, sec level, IP address of the VLAN.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface 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	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was changed.
3.1(1)	This command was modified to change arguments to be separate commands under interface configuration mode.

Usage Guidelines

In multimode in the system, you can allocate interfaces to context which allows the FWSM to add them; you do not need to manually add interfaces. Similarly, if you assign a VLAN to the failover or state link, the **interface** command is added automatically.

In single mode, you need to enter the interface command for a given VLAN, to set parameters for it.

In interface configuration mode, you can assign a name, assign a VLAN, assign an IP address, and configure many other settings. If you add an interface for a VLAN that is not yet assigned to the FWSM by the switch, the interface will be in the down state. When you assign the VLAN to the FWSM, the interface changes to an up state. See the **show interface** command for more information about interface states.

When you assign a VLAN to a context using the **allocate-interface** command, the FWSM automatically adds the interface to the system configuration, if it is not already present. For example, when you allocate 'VLAN 100' to a context, the **interface vlan 100** command is added to the system configuration.

The **failover lan interface** *interface_name* **vlan** *vlan* command specifies the interface name and the VLAN used for communication between the active and the standby modules to determine the operating status of each module.

The **failover link** *interface_name* [**vlan** *vlan*] command specifies the interface name and VLAN for the stateful failover interface. The link passes all protocol state information between the active and the standby for stateful failover.

Examples

The following example shows how to enter the interface configuration mode:

```
fws(config-if)# interface vlan22  
fws(config-if)# shutdown
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears all configuration for an interface.
clear interface	Clears counters for the show interface command.
show interface	Displays the runtime status and statistics of interfaces.

interface bvi

To configure the bridge virtual interface for a bridge group, use the **interface bvi** command in global configuration mode. To remove the bridge virtual interface configuration, use the **no** form of this command. Use this command to enter interface configuration mode so you can configure a management IP address for the bridge group.

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

Syntax Description

bridge_group_number Specifies the bridge group number as an integer between 1 and 100.

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
3.1(1)	This command was introduced.

Usage Guidelines

A transparent firewall connects the same network on its inside and outside interfaces. Each pair of interfaces belongs to a bridge group, to which you must assign a management IP address. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.

Assign each interface to a bridge group using the **interface vlan** command, and then the **bridge-group** command. Use the **interface bvi** command, and then the **ip address** command to configure the management IP address for the bridge group. The management IP address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, such as system messages or communications with AAA servers. You can also use this address for remote management access.

Examples

The following example assigns VLANs 300 and 301 to bridge group 1, then sets the management address and standby address of bridge group 1:

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
```

```
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

Command	Description
bridge-group	Groups two transparent firewall interfaces into a bridge group.
clear configure interface bvi	Clears the bridge virtual interface configuration.
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.
show running-config interface bvi	Shows the bridge group interface configuration.

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

<i>num</i>	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
<i>%</i>	(Optional) Specifies that the number <i>num</i> 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:

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

Command History

Release	Modification
3.1(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 FWSM is functioning properly, the FWSM will mark itself as failed and a failover may occur (if the active FWSM 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.

ip address

To set the IP address for an interface (in routed mode) or the management address for a bridge group (transparent mode), use the **ip address** command in interface configuration mode. For routed mode, enter interface configuration mode for the VLAN ID (the **interface** command). For transparent mode, enter interface configuration mode for the bridge group (the **interface bvi** command). 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

<i>ip_address</i>	Sets the IP address for the interface (routed mode) or the management IP address for the bridge group (transparent mode).
<i>mask</i>	(Optional) Sets the subnet mask for the IP address. If you do not set the mask, the FWSM uses the default mask for the IP address class. Do not assign a host address (/32 or 255.255.255.255) to the transparent firewall. Also, do not use other subnets that contain fewer than 3 host addresses (one each for the upstream router, downstream router, and transparent firewall) such as a /30 subnet (255.255.255.252). The FWSM drops all ARP packets to or from the first and last addresses in a subnet. For example, if you use a /30 subnet and assign a reserved address from that subnet to the upstream router, then the FWSM drops the ARP request from the downstream router to the upstream router.
standby <i>ip_address</i>	(Optional) Sets the IP address for the standby unit for failover. The standby IP address must be on the same subnet as the main IP address.

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
Interface configuration	•	•	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	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.

In transparent firewall mode, each pair of interfaces belongs to a bridge group, to which you must assign a management IP address. Each bridge group connects to a separate network. The management IP address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, 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. The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface vlan 100
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)# interface vlan 200
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
```

The following transparent firewall example assigns VLANs 300 and 301 to bridge group 1, then sets the management address and standby address of bridge group 1:

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

Command	Description
interface bvi	Configures a transparent firewall bridge group.
bridge-group	Assigns an interface to a bridge group.
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 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

<i>first-address</i>	Specifies the starting address in the range of IP addresses.
<i>last-address</i>	Specifies the final address in the range of IP addresses.
mask <i>mask</i>	(Optional) Specifies a subnet mask for the pool of addresses.
<i>poolname</i>	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:

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

Command History

Release	Modification
3.1(1)	Support for 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 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Normally, the FWSM only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the FWSM 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 FWSM, the FWSM routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the FWSM 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 FWSM 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 FWSM drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the FWSM 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.

ip-address

To include the FWSM IP address in the certificate during enrollment, use the **ip-address** command in `crypto ca trustpoint` configuration mode. To restore the default setting, use the **no** form of the command.

ip-address *ip-address*

no ip-address

Syntax Description	<i>ip-address</i>	Specifies the IP address of the FWSM.

Defaults	The default setting is to not include the IP address.

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 configuration	•	•	•	•	—

Release	Modification
3.1(1)	This command was introduced.

Examples	The following example enters <code>crypto ca trustpoint</code> configuration mode for <code>trustpoint central</code> , and includes the FWSM IP address in the enrollment request for <code>trustpoint central</code> :

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# ip-address 209.165.200.225
```

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

ip-address-privacy

To enable the IP Address Privacy feature, use the `ip-address-privacy` command in SIP map configuration mode. To disable IP Address Privacy, use the **no** form of this command.

ip-address-privacy

no ip-address-privacy

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
SIP map configuration	•	•	•	•	—

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

When IP Address Privacy is enabled, if any two SIP endpoints participating in an IP phone call or instant messaging session use the same internal firewall interface to contact their SIP proxy server on an external firewall interface, all SIP signaling messages go through the SIP proxy server.

IP Address Privacy can be enabled when SIP over TCP or UDP application inspection is enabled. By default, this feature is disabled. If IP Address Privacy is enabled, the FWSM does not translate internal and external host IP addresses embedded in the TCP or UDP payload of inbound SIP traffic, ignoring translation rules for those IP addresses.

Examples

The following example shows how to identify SIP traffic, define a SIP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map s1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sip	Enables SIP application inspection.
policy-map	Associates a class map with specific security actions.
sip-map	Defines a SIP application inspection map.

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:

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

Command History

Release	Modification
3.1(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 FWSM. 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 nbar protocol-tagging (IOS)

If you use Programmable Intelligent Services Accelerator (PISA) integration with the FWSM, then to enable the PISA to tag packets with an application type using GRE, use the **ip nbar protocol-tagging** command in interface configuration mode. To disable tagging, use the **no** form of this command.



Note

This feature depends on Cisco IOS Release 12.2(18)ZYA, and will not be supported on the FWSM until the Cisco IOS software is released.

ip nbar protocol-tagging [**vlan-list** *vlan_list*]

no ip nbar protocol-tagging [**vlan-list** *vlan_list*]

Syntax Description

vlan-list <i>vlan_list</i>	(Optional) If you want to enable tagging on a trunk port and want to limit tagging to particular VLANs, enter a list of VLANs. By default, all VLANs are tagged. The <i>vlan_list</i> can be one or more VLANs identified in one of the following ways: • A single number (<i>n</i>) • A range (<i>n-x</i>) Separate numbers or ranges by commas. For example, enter the following numbers: 5,7-10,13,45-100

Defaults

No default behavior or values.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2(18)ZYA	This command was introduced.

Usage Guidelines

Before you enable protocol tagging, you must enable classification using the **ip nbar protocol-discovery** command. See the Cisco IOS documentation for more information about NBAR classification.

The PISA on the switch supervisor can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type. Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to configure multiple upstream switches with PISAs installed.

You might want to deny certain types of application traffic when you want to preserve bandwidth for critical application types. For example, you might deny the use of peer-to-peer (P2P) applications if they are affecting your other critical applications.

After the PISA identifies the application used by a given traffic flow, it encapsulates all packets using GRE and includes a tag informing the FWSM of the application type. In addition, an outer IP header almost identical (except for the Layer 4 protocol, which now indicates GRE) to the inner/original IP header is added. The original Layer 2 header is maintained. This preserves the original routing/switching paths for the modified packet. The GRE encapsulation adds 32 bytes (20 bytes for the outer IP header and 12 bytes for the GRE header).

After the FWSM receives the packet and acts on the information, it strips the GRE encapsulation from the packet.

When you configure the FWSM to deny traffic based on the PISA encapsulation, for the VLAN on which that traffic resides, the PISA encapsulates all traffic (including traffic that you did not specify for denial).

The GRE encapsulation increases the packet size slightly, so you should increase the MTU between the PISA and the FWSM according to the Cisco IOS **mtu** and **system jumbomtu** commands.

The GRE encapsulation causes a slight performance impact for PISA traffic sent to the FWSM.



Note

Classification (the **ip nbar protocol-discovery** command) and tagging need to be enabled on the same port; for example, you cannot enable classification on an access ports and tagging on a trunk port.

Examples

The following example enables protocol discovery and tagging on an SVI:

```
Router(config)# interface vlan 100
Router(config-if)# ip nbar protocol-discovery
! enables discovery
Router(config-if)# ip nbar protocol-tagging
! enables tagging
Router(config-if)# mtu 9216
! Allows packet sizes up to 9216 bytes without fragmenting
```

The following example enables protocol discovery and tagging on uplink port GigabitEthernet 6/1:

```
Router(config)# interface gigabitethernet 6/1
Router(config-if)# ip nbar protocol-discovery
! Classification
Router(config-if)# ip nbar protocol-tagging vlan-list 100
! Tagging
Router(config-if)# mtu 9216
! Allow packet size up to 9216 bytes without fragmenting
Router(config)# system jumbomtu 9216
! Set global LAN port MTU to 9216 bytes
```

Related Commands

Command	Description
show ip nbar protocol-tagging	Shows tagging configuration information.

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:

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

Command History

Release	Modification
3.1(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 FWSM before connecting.

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 FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM 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 FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM that is running NAT.

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 FWSM 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.
<i>destination-ipv6-address</i>	The IPv6 address of the host receiving the traffic.
<i>destination-ipv6-prefix</i>	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 FWSM.

<i>icmp_type</i>	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 <i>icmp_type</i> argument indicates all ICMP types.
<i>icmp_type_obj_grp_id</i>	(Optional) Specifies the object group ICMP type ID.
<i>id</i>	Name or number of an access list.
interval <i>secs</i>	(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.
<i>level</i>	(Optional) Specifies the syslog level for message 106100; valid values are from 0 to 7. The default level is 6 (informational).
line <i>line-num</i>	(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 specify 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.
<i>network_obj_grp_id</i>	Existing network object group identification.
object-group	(Optional) Specifies an object group.

<i>operator</i>	(Optional) Specifies the operand to compare the source IP address to the destination IP address. The <i>operator</i> 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.
<i>port</i>	(Optional) Specifies the port that you permit or deny access. When entering the <i>port</i> argument, you can specify the port by either a number in the range of 0 to 65535 or a using literal name if the <i>protocol</i> is tcp or udp. Permitted TCP literal names are aol, bgp, chargen, cifs, 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 xmcp.
<i>prefix-length</i>	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
<i>protocol</i>	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.
<i>protocol_obj_grp_id</i>	Existing protocol object group identification.
<i>service_obj_grp_id</i>	(Optional) Specifies the object group.
<i>source-ipv6-address</i>	The IPv6 address of the host sending the traffic.
<i>source-ipv6-prefix</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command lets you 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 FWSM 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, see the **access-list extended** command.

The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the FWSM. 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 FWSM.
object-group	Creates an object group (addresses, ICMP types, and services).

ipv6 access-list remark

To add a remark to an IPv6 access list, use the **ipv6 access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

ipv6 access-list *id* [**line** *line-num*] **remark** *text*

no ipv6 access-list *id* [**line** *line-num*] **remark** [*text*]

Syntax Description

<i>id</i>	The name of an IPv6 access list.
line <i>line-num</i>	(Optional) The line number at which to insert the remark.
remark <i>text</i>	The text of the remark.

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
3.1(1)	This command was introduced.

Usage Guidelines

The remark text can be up to 100 characters in length, including spaces and punctuation. If you enter more than 100 characters, the remark is truncated at the 100th character. The remark text must contain at least 1 non-space character; you cannot enter an empty remark. You can enter more than one remark for each access list.

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 the remark to add before or after an **ipv6 access-list** command:

```
hostname(config)# ipv6 access-list example remark this access list should not be used
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
clear configure ipv6 access-list	Clears the IPv6 access lists from the running configuration.
ipv6 access-list	Adds an IPv6 access list to the configuration.
show ipv6 access-list	Displays the IPv6 access lists.
show running-config ipv6	Displays the ipv6 commands in the running configuration.

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.
<i>ipv6-address</i>	The IPv6 link-local address assigned to the interface.
<i>ipv6-prefix</i>	The IPv6 network address assigned to the interface.
link-local	Specifies that the address is a link-local address.
<i>prefix-length</i>	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:

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

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# ipv6 address 3ffe:c00:0:1::576/64
```

The following example assigns an IPv6 address automatically for the selected interface:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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 Vlan101
hostname(config-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 Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# 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 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 <code>::/0</code> .
deny		Prevents the specified ICMP traffic on the selected interface.
host		Indicates that the address refers to a specific host.
<i>icmp-type</i>		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: • echo • echo-reply • membership-query • membership-reduction • membership-report • neighbor-advertisement • neighbor-redirect • neighbor-solicitation • destination-unreachable • packet-too-big • parameter-problem • router-advertisement • router-renumbering • router-solicitation • time-exceeded • unreachable
<i>if-name</i>		The name of the interface, as designated by the nameif command, the access rule applies to.
<i>ipv6-address</i>		The IPv6 address of the host sending ICMPv6 messages to the interface.
<i>ipv6-prefix</i>		The IPv6 network that is sending ICMPv6 messages to the interface.
permit		Allows the specified ICMP traffic on the selected interface.
<i>prefix-length</i>		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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM 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
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

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

<i>value</i>	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:

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

Command History

Release	Modification
3.1(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:

```
%fwm-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:

```
%fwm-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 Vlan101  
hostname(config-subif)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
hostname(config)# interface Vlan101  
hostname(config-subif)# 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

<i>value</i>	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:

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

Command History

Release	Modification
3.1(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 Vlan101:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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		
<i>at valid-date preferred-date</i>		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 <i>date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire</i> .
default		Default values are used.
infinite		(Optional) The valid lifetime does not expire.
<i>ipv6-prefix</i>		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.
<i>preferred-lifetime</i>		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).
<i>prefix-length</i>		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.
<i>valid-lifetime</i>		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		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	•	—	•	•	—

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# 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.
<i>value</i>	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:

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

Command History

Release	Modification
3.1(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 FWSM 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 Vlan101
hostname(config-subif)# 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 FWSM as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM as a default router on this interface.

Setting the value to a non-zero value indicates that the FWSM should be considered a default router on this interface. The non-zero value for the “router lifetime” value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the FWSM 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 Vlan101
hostname(config-subif)# 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

<i>value</i>	The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default is 0.

Defaults

0 milliseconds.

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
Interface configuration	•	—	•	•	—

Command History

Release	Modification
3.1(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.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# 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

<i>if_name</i>	The internal or external interface name designated by the nameif command.
<i>ipv6_address</i>	The IPv6 address that corresponds to the local data-link address.
<i>mac_address</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	—	•	•	—

Command History

Release	Modification
3.1(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 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*]

no ipv6 route *if_name* *ipv6-prefix/prefix-length* *ipv6-address* [*administrative-distance*]

Syntax Description

<i>administrative-distance</i>	(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.
<i>if_name</i>	The name of the interface the route is being configured for.
<i>ipv6-address</i>	The IPv6 address of the next hop that can be used to reach the specified network.
<i>ipv6-prefix</i>	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.
<i>prefix-length</i>	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

By default, the *administrative-distance* is 1.

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
3.1(1)	This command was introduced.

Usage Guidelines

Use the **show ipv6 route** command to view the contents of the IPv6 routing table.

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.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

Examples The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# isakmp disconnect-notify
```

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.

Related Commands

isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM, 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:

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

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

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 <i>key_id_string</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.
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 <i>seconds</i>	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 <i>seconds</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access and IPSec LAN-to-LAN tunnel-group types only.

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 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-ipsec)# isakmp keepalive threshold 15 retry 10
```

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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 reset the authentication method to the default value, use the **no** form of this command.

isakmp policy *priority* authentication {pre-share | dsa-sig | rsa-sig}

no isakmp policy *priority* authentication

Syntax Description

dsa-sig	Specifies DSA signatures 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If you specify RSA signatures, you must configure the FWSM 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 FWSM 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.
<i>priority</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

[no] isakmp policy priority group {1 | 2 | 5 | 7}

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.
group 7	Specifies that Diffie-Hellman Group 7 be used in the IKE policy. Group 7 generates IPsec SA keys, where the elliptical curve field size is 163 bits.
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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

There are four group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), 1536-bit (DH Group 5), and DH Group 7. 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 be used within the IKE policy with the priority number of 40.

```
hostname(config-if)# 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.
<i>priority</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

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. You can specify an infinite lifetime if the peer does not propose a lifetime. 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

<i>priority</i>	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.
<i>seconds</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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.

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 50,400 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 FWSM, 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 FWSM, 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, tells the FWSM 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-name

To identify the DN from the CA certificate to be compared to the rule entry string, use the **issuer-name** command in CA certificate map configuration mode. To remove an issuer-name, use the **no** form of the command.

issuer-name [**attr tag**] {**eq** | **ne** | **co** | **nc**} *string*

no issuer-name [**attr tag**] {**eq** | **ne** | **co** | **nc**} *string*

Syntax Description	attr tag	Indicates that only the specified attribute value form the certificate DN string 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 DN string or indicated attribute must be a substring in the rule entry string.
	eq	Specifies that the DN string or indicated attribute must match the entire rule string.
	nc	Specifies that the DN string or indicated attribute must not be a substring in the rule entry string.
	ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
	<i>string</i>	Specifies the rule entry information.

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
CA certificate map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters the CA certificate map mode for certificate map 4 and configures the issuer name as O = central:

```
hostname(config)# crypto ca certificate map 4
hostname(ca-certificate-map)# issuer-name attr o eq central
hostname(ca-certificate-map)# exit
```

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.



CHAPTER

17

join-failover-group through kill Commands

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:

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

Command History

Release	Modification
3.1(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.

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

<i>string</i>	A case-sensitive, alphanumeric string, up to 64 characters long. Spaces are not permitted in the string.
Note	Kerberos realms only use numbers and upper-case letters. Although the FWSM accepts lower-case letters in the <i>string</i> 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:

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

Command History

Release	Modification
3.1(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 FWSM does not translate lower-case letters to upper-case letters.

Examples

The following sequence shows the **kerberos-realm** command used 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
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so that 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 FWSM to the AAA server, use the **key** command in aaa-server host mode. Aaa-server host configuration mode is accessible 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:

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

Command History

Release	Modification
3.1(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.

This command is valid only for RADIUS and TACACS+ servers.

The **key** parameter of the **aaa-server** command in earlier FWSM versions is automatically converted to the equivalent **key** command.

Examples

The following example configures a TACACS+ 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 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 that 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

<i>name</i>	Specifies 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:

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

Command History

Release	Modification
3.1(1)	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.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM.
who	Displays a list of active Telnet sessions.



CHAPTER

18

Idap-base-dn through log-adj-changes Commands

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 accessible 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

<i>string</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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 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 that 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

<i>port</i>	(Optional) Specifies the LDAP server port. If this parameter is not specified, the FWSM uses the standard LDAP port (389).
<i>server</i>	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:

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

Command History

Release	Modification
3.1(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

<i>password</i>	Defines a password for this distinguished name. The maximum field length is 128 characters.
<i>x.500-name</i>	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:

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

Command History

Release	Modification
3.1(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.

Command	Description
crypto ca trustpoint	Enters ca trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.

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 mode. Aaa-server host configuration mode is accessible 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:

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

Command History

Release	Modification
3.1(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 FWSM establish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The FWSM 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 FWSM. 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 a RADIUS 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)# exit

```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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 mode. Aaa-server host configuration mode is accessible 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:

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

Command History

Release	Modification
3.1(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 a RADIUS 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 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)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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 (or attributes), use the **ldap-naming-attribute** command in aaa-server host mode. Aaa-server host configuration mode is accessible 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

<i>string</i>	The case-sensitive, alphanumeric Relative Distinguished Name attribute (or attributes), 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	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Enter the Relative Distinguished Name attribute (or attributes) 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 a RADIUS 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 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)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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-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 accessible 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 a RADIUS 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-serve-host)# ldap-scope subtree  
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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 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.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This feature does not work as intended if you enable interactive hardware client authentication.

For further information, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.



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 FWSM before connecting.

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 FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

limit-resource {**all** [*number*% | **0**] | [**rate**] *resource_name* *number*[%] | **0**}

no limit-resource {**all** | [**rate**] *resource_name*}

Syntax Description

0	Sets the resource to unlimited (the system limit).
all	Sets the limit for all resources, as a percentage, or as unlimited.
<i>number</i> [%]	Specifies the resource limit as a fixed number greater than or equal to 1, or as a percentage of the system limit (when used with the percent sign (%)). You can assign more than 100 percent if you want to oversubscribe the device. For all resources, you can only set a percentage or 0 for unlimited.
rate	Specifies that you want to set the rate per second for a resource for which you can set either the rate or an absolute limit. See Table 18-1 for resources for which you can set the rate per second.
<i>resource_name</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Class configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

When you limit a resource for a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM 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	Minimum and Maximum Number per Context	Total Number for System	Description
mac-addresses	N/A	65 K concurrent	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	N/A	999,900 concurrent 102,400 per second (rate)	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. Note For concurrent connections, the FWSM allocates half of the limit to each of two network processors (NPs) that accept connections. Typically, the connections are divided evenly between the NPs. However, in some circumstances, the connections are not evenly divided, and you might reach the maximum connection limit on one NP before reaching the maximum on the other. In this case, the maximum connections allowed is less than the limit you set. The NP distribution is controlled by the switch based on an algorithm. You can adjust this algorithm on the switch, or you can adjust the connection limit upward to account for the inequity.
fixups	N/A	10,000 per second (rate)	Application inspection.
hosts	N/A	256 K concurrent	Hosts that can connect through the FWSM.
ipsec	1 minimum 5 maximum concurrent	10 concurrent	IPSec sessions
asdm	1 minimum 5 maximum concurrent	32 concurrent	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	1 minimum 5 maximum concurrent	100 concurrent	SSH sessions.

Table 18-1 Resource Names and Limits (continued)

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
syslogs	N/A	30,000 per second (rate)	System messages. Note The FWSM can support 30,000 messages per second for messages sent to the FWSM terminal or buffer. If you send messages to a syslog server, the FWSM supports 25,000 per second.
telnet	1 minimum 5 maximum concurrent	100 concurrent	Telnet sessions.
xlates	N/A	256 K concurrent	NAT translations.

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 with all resources set to 5 percent, except for fixups, with a setting of 10 percent, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

To add a class called silver with all resources set to 3 percent, except for system log messages, with a setting of 500 per second, enter the following commands:

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

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.

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. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. This log action is available in an inspection policy map 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:

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

Release	Modification
4.0(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 Commands

logging asdm

To send syslog messages to ASDM, use the **logging asdm** command in global configuration mode. To disable logging to ASDM, use the **no** form of this command.

logging asdm [*message_list* | *level*]

no logging asdm [*message_list* | *level*]

Syntax Description

<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog 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.
<i>message_list</i>	Specifies the name of the list that identifies the messages to be sent to ASDM. 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Before any messages are sent to ASDM, you must enable system logging using the **logging enable** command.

When the ASDM log buffer is full, the FWSM deletes the oldest message to make room in the buffer for new messages. To control the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command.

The ASDM log buffer is a different buffer than the internal log buffer enabled by the **logging buffered** command. The FWSM only places messages in the ASDM log buffer if they are destined to be sent to ASDM.

Examples

The following 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 of the syslog messages it contains.
logging asdm-buffer-size	Specifies the number of ASDM messages retained in the ASDM log buffer.

logging asdm-buffer-size

To specify the number of syslog 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	<i>num_of_msgs</i>	Specifies the number of syslog messages that the FWSM 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:

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

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When the ASDM log buffer is full, FWSM 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 syslog messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the internal log buffer enabled by the **logging buffered** command. The FWSM only places messages in the ASDM log buffer if they are destined to be sent to ASDM.

Examples

The following 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 of the syslog messages it contains.
logging asdm	Enables logging to the ASDM log buffer.
logging enable	Enables logging to all specified output locations.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffered

To enable the FWSM to save syslog messages in 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 [*message_list* | *level*]

no logging buffered [*message_list* | *level*]

Syntax Description	<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity 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.
	<i>message_list</i>	Specifies the list that identifies the messages to send to the internal log buffer. For information about creating message lists, see the logging list command.

Defaults	The defaults are as follows: • Logging to the internal log buffer is disabled. • Log buffer size is 4 KB.

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
	3.1(1)	This command was introduced.

Usage Guidelines

For the FWSM to generate syslog messages, you must enable logging using the **logging enable** command. Use the **logging buffered** command to specify the internal log buffer as an output destination.

The FWSM appends new messages to the end of the log buffer. When the log buffer is full, it “wraps” to the first message in the buffer. Unless configured otherwise, the FWSM writes over messages, oldest message first, when new messages are generated.

You can configure the FWSM so that the log buffer content is automatically saved each time the buffer wraps. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

In addition, you can save the buffer contents at any time to internal flash memory. For more information, see the **logging savelog** command.

Syslog messages in the internal buffer can be viewed with the **show logging** command.

Examples

The following example configures logging to the buffer for level 0 and level 1 events:

```
hostname(config)# logging buffered alerts
hostname(config)#
```

The following example creates a list named notif-list with a maximum logging level of 7 and configures logging to the buffer for syslog messages identified by the notif-list message list that you created.

```
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 syslog messages it contains.
logging buffer-size	Specifies log buffer size.
logging flash-bufferwrap	Writes the log buffer to internal flash memory when the log buffer wraps.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer wraps.
logging list	Creates a reusable list of message selection criteria.
logging savelog	Saves the contents of the log buffer to internal flash memory.

logging buffer-size

To specify the size of the system log buffer, use the **logging buffer-size** command in global configuration mode. To reset the system 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	<i>bytes</i>	Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the FWSM 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:

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

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To see whether the FWSM 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 is not shown, then the FWSM uses a log buffer size of 4 KB.

For more information about how the FWSM uses the system log buffer, see the **logging buffered** command.

Examples

This example enables system logging, enables the system log buffer as a log output destination, and specifies that the FWSM 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 syslog messages it contains.
logging buffered	Enables logging to the system log buffer.
logging flash-bufferwrap	Writes the contents of the system log buffer to internal flash memory when the log buffer wraps.
logging savelog	Saves the contents of the log buffer to internal flash memory.
show logging	Displays the contents of the internal log buffer and the enabled logging options.

logging class

To specify an output destination for an entire class of messages, use the **logging class** command in global configuration mode. To remove the output destination for a messages class, use the **no** form of the command.

logging class *message_class* *output_destination* [*severity_level*]

no logging class *class*

Syntax Description

<i>class</i>	Specifies the message class to be sent to the specified output destination. For valid values of <i>class</i> , see the “Usage Guidelines” section that follows.
<i>destination</i>	Specifies a log output destination for <i>class</i> . For valid values of <i>output_destination</i> , see the “Usage Guidelines” section that follows.
<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity 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 FWSM 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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Valid values for *class* are as follows:

- **auth**—User authentication
- **bridge**—Transparent firewall
- **ca**—PKI certificate authority
- **config**—Command interface
- **email**—Email proxy
- **ha**—Failover
- **ids**—Intrusion detection system
- **ip**—IP stack
- **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

The following 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 syslog buffer is 7:

```
hostname(config)# logging class ha asdm 2 buffered 7
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 console

To enable the FWSM to display syslog messages in console sessions, use the **logging console** command in global configuration mode. To disable the display of syslog messages in console sessions, use the **no** form of this command.

logging console [*message_list* | *level*]

no logging console



Note

We recommend that you do not use this command because it may cause many syslog messages to be dropped due to buffer overflow. For more information, see the “Usage Guidelines” section that follows.

Syntax Description

<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog 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.
<i>message_list</i>	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 FWSM does not display syslog messages in console sessions 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
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the console, you must enable system logging using the **logging enable** command.

**Caution**

Using the **logging console** command could drastically degrade system performance. Instead, use the **logging buffered** command to designate the internal log buffer as an output destination, then use the **show logging** command to see 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 syslog messages of severity 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 to all specified output destinations.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the contents of the internal log buffer and 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 such as syslog message 711011 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 FWSM does not include debugging output in syslog messages.

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
3.1(1)	This command was introduced.

Usage Guidelines

Debugging messages are generated as severity level 7 messages. They appear in logs with the syslog message number 711011.

Examples

The following example shows how to enable logging, send log messages to the 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:

```
%FWSM-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging to all output destinations.
show logging	Displays the contents of the internal log buffer and the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging deny-conn-queue-full

To prevent the creation of new transit connections through the FWSM when the logging queue is full, use the **logging deny-conn-queue-full** command in global configuration mode. To allow the creation of new transit connections through the FWSM when the logging queue is full, use the **no** form of this command.

logging deny-conn-queue-full

no logging deny-conn-queue-full

Syntax Description

deny-conn-queue-full This option does not allow the creation of new transit connections through the FWSM when the logging queue is full.

Note If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages).

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
3.1(1)	This command was introduced.

Usage Guidelines

When traffic is so heavy that the logging queue fills up, the FWSM might discard messages. You can prevent the creation of new transit connections through the FWSM to avoid discarding messages.

Examples

The following example shows how to display the output of the **logging deny-conn-queue-full** and **show logging queue** commands:

```
hostname(config)# logging deny-conn-queue-full
hostname(config)# show logging queue

Logging Queue length limit: Unlimited
1 msg(s) discarded due to queue overflow
Current 5 msgs on queue, 3513 msgs most on queue
```

In this example, the **logging deny-conn-queue-full** command prevents the creation of new transit connections through the FWSM when the logging queue is full. The syslog messages currently in the queue are processed by the FWSM in the manner specified by the current logging configuration, such as sending syslog messages to e-mail recipients, saving buffer overflows to internal flash memory, and so on. The logging queue does not discard any messages.

The sample output of the **show logging queue** command shows the following:

- Five messages are queued.
- The largest number of messages in the queue at one time since the FWSM was last booted was 3513.
- One message was discarded.

Even though the queue length was set for unlimited, a message was discarded because no block memory was available to add the message to the queue.

Related Commands	Command	Description
	logging queue	Specifies how many syslog messages that the FWSM can hold in its system log queue before processing them.
	show logging queue	Displays syslog messages currently in the logging queue.

logging device-id

To configure the FWSM to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the inclusion of a device ID in messages, 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	Use the name of the current context as the device ID.
hostname	Use the hostname of the FWSM as the device ID.
ipaddress <i>interface_name</i>	Use as the device ID the IP address of the interface specified as <i>interface_name</i> . If you use the ipaddress keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the FWSM uses to send the log data to the external server.
string <i>text</i>	Use as the device ID the characters contained in <i>text</i> , which can be up to 16 characters long. You cannot use white space characters or any of the following characters in <i>text</i> : • &—ampersand • '—single quote • "—double quote • <—less than • >—greater than • ?—question mark

Defaults

No default device ID is used in syslog messages.

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
3.1(1)	This command was introduced.

Usage Guidelines

If you use the **ipaddress** keyword, the device ID becomes the specified FWSM 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

The following example shows how to specify a device ID of secappl-1 and the output from the **show logging** command:

```
hostname(config)# logging device-id secappl1
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"
```

In syslog messages, the hostname secappl-1 appears at the beginning of the message, such as the following:

```
secappl-1 %FWSM-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

Related Commands

Command	Description
logging enable	Enables logging to all specified output destinations.
show logging	Displays contents of the internal log buffer and 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 syslog messages that are sent to output destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of the 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 FWSM does not use EMBLEM format for syslog messages.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **logging emblem** command enables you to configure the FWSM to use the EMBLEM-format for all messages being sent to output destinations other than to syslog servers; specifically, messages sent to one or more e-mail addresses, the internal log buffer, ASDM, a Telnet session, or an SNMP management station use the EMBLEM-format. If you also enable the **logging timestamp** keyword, the messages also include a timestamp.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

Examples

The following 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.
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 FWSM to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the inclusion of a device ID in messages, 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	Use the name of the current context as the device ID.
hostname	Use the hostname of the FWSM as the device ID.
ipaddress <i>interface_name</i>	Use as the device ID the IP address of the interface specified as <i>interface_name</i> . If you use the ipaddress keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the FWSM uses to send the log data to the external server.
string <i>text</i>	Use as the device ID the characters contained in <i>text</i> , which can be up to 16 characters long. You cannot use white space characters or any of the following characters in <i>text</i> : • &—ampersand • '—single quote • "—double quote • <—less than • >—greater than • ?—question mark

Defaults

No default device ID is used in syslog messages.

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
3.1(1)	This command was introduced.

Usage Guidelines

If you use the **ipaddress** keyword, the device ID becomes the specified FWSM 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

The following example shows how to specify a device ID of secappl-1 and the output from the **show logging** command:

```
hostname(config)# logging device-id secappl1
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"
```

In syslog messages, the hostname secappl-1 appears at the beginning of the message, such as the following:

```
secappl-1 %FWSM-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

Related Commands

Command	Description
logging enable	Enables logging to all specified output destinations.
show logging	Displays contents of the internal log buffer and 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 system message 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 system log 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

System log servers file messages based on the *facility* number in the message. There are eight possible facilities, 16 (LOCAL0) through 23 (LOCAL7).

Examples

The following example shows how to set the logging facility as 16. The output of the **show logging** command includes the facility being used by the FWSM in syslog messages.

```
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 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 configure the FWSM to write the contents of the log buffer to internal flash memory every time the buffer wraps, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing the contents of the log buffer to internal 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:

- Log buffer is not specified as an output destination.
- Writing the contents of the log buffer to internal flash memory is disabled.
- Log buffer size is 4 KB.
- Minimum free internal flash memory is 3 MB.
- Maximum internal flash memory allocation for buffer logging is 1 MB.

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
3.1(1)	This command was introduced.

Usage Guidelines

For the FWSM to write the log buffer contents to internal flash memory when the buffer wraps, you must first configure the log buffer as an output destination; otherwise, the log buffer remains empty. To configure the log buffer as an output destination, use the **logging buffered** command.

While the FWSM writes the log buffer contents to internal flash memory, it continues storing to the log buffer any new event messages.

The FWSM 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 internal flash memory affects how the FWSM saves logs using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

Examples

The following example shows how to enable system logging, specify the log buffer as an output destination, and enable the FWSM to write the log buffer contents to internal flash memory when the buffer wraps:

```
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.
logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer.
logging buffer-size	Specifies the log buffer size.
logging flash-maximum-allocation	Specifies the maximum amount of internal flash memory that can be used for logs.
logging flash-minimum-free	Specifies the minimum amount of internal flash memory that must be available for the FWSM to permit writing the log buffer contents to internal flash memory.
show logging	Displays the enabled logging options.

logging flash-maximum-allocation

To specify the maximum amount of internal flash memory that the FWSM uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. This command determines how much internal flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands. To reset the maximum amount of internal flash memory used for this purpose to its default size of 1 MB, 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 internal flash memory, in kilobytes, that the FWSM can use to save log buffer data.

Defaults

The default maximum internal flash memory allocation for log data is 1 MB.

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
3.1(1)	This command was introduced.

Usage Guidelines

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** requires more internal flash memory than the maximum amount specified by the **logging flash-maximum-allocation** command, the FWSM 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 FWSM fails to save the new log file.

To determine whether the FWSM has a maximum internal 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 FWSM uses a maximum of 1 MB for log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the FWSM uses the log buffer, see the **logging buffered** command.

Examples

This example shows how to enable logging, specify the log buffer as an output destination, enable the FWSM to write the log buffer contents to internal flash memory, with the maximum amount of internal flash memory used for log data 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
logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
logging flash-bufferwrap	Enables the log buffer contents to be written to internal flash memory when the log buffer wraps.
logging flash-minimum-free	Specifies the minimum amount of internal flash memory that must be available for the FWSM to permit writing the log buffer contents to internal flash memory.
logging savelog	Saves the contents of the log buffer to internal flash memory each time the command is entered at the command line.

logging flash-minimum-free

To specify the minimum amount of free internal flash memory that must exist before the FWSM saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. This command affects how much free internal flash memory must exist before the FWSM saves log files created by the **logging savelog** and **logging flash-bufferwrap** commands. To reset the minimum required amount of free internal 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 internal flash memory, in kilobytes, that must be available before the FWSM saves a new log file.

Defaults

The default minimum free internal flash memory is 3 MB.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **logging flash-minimum-free** command specifies how much internal 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 internal flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the FWSM 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 FWSM fails to save the new log file.

Examples

The following example shows how to specify that the minimum amount of free internal flash memory must be 4000 KB:

```
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

Related Commands	Command	Description
	logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
	logging flash-bufferwrap	Writes the log buffer to internal flash memory when the log buffer wraps.
	logging flash-maximum-allocation	Specifies the maximum amount of internal flash memory that can be used for log data.
	logging saveolog	Saves the contents of the log buffer to internal flash memory each time the command is entered at the command line.

logging from-address

To specify the source e-mail address for syslog messages e-mailed by the FWSM, use the **logging from-address** command in global configuration mode. This e-mail address appears in the From: line of all e-mailed syslog messages. To remove the source 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 appears in the From: line of each e-mailed syslog message.

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
3.1(1)	This command was introduced.

Usage Guidelines

Sending syslog 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

The following example shows how set up the FWSM to send a limited number of syslog messages by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the address from whom messages are sent.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according to the example criteria, 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 mail	Enables the FWSM to send syslog messages by e-mail and specifies which messages are sent by e-mail.
	logging recipient-address	Specifies the e-mail address to which e-mailed syslog messages are sent.
	smtp-server	Configures an SMTP server.

logging ftp-bufferwrap

To enable the FWSM to write the contents of the log buffer to an FTP server every time the buffer wraps, use the **logging ftp-bufferwrap** command in global configuration mode. To disable writing the contents of 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable **logging ftp-bufferwrap**, the FWSM sends log buffer data to the FTP server every time the log buffer wraps. You specify the FTP server to be sent the log buffer data with the **logging ftp-server** command.

For the FWSM to send the log buffer contents to the FTP server when the buffer wraps, you must first configure the log buffer as an output destination; otherwise, the log buffer remains empty. To configure the log buffer as an output destination, use the **logging buffered** command.

While the FWSM sends log data to the FTP server, it continues storing new messages to the log buffer.

The FWSM 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

The following example shows how to enable the log buffer, specify an FTP server, and enable the FWSM to write the log buffer contents to an FTP server each time the buffer wraps. 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 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 syslog messages it contains.
logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
logging buffer-size	Specifies log buffer size.
logging ftp-server	Specifies FTP server parameters for use with the logging ftp-bufferwrap command.

logging ftp-server

To specify details about the FTP server the FWSM 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 ftp_server path username password*

no logging ftp-server *ftp-server ftp_server path username password*

Syntax Description

<i>ftp-server</i>	External FTP server IP address or hostname. Note If you specify a hostname, be sure DNS is operating correctly on your network.
<i>password</i>	The password for the username specified.
<i>path</i>	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: <i>/security_appliances/syslogs/appliance107</i>
<i>username</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM does not verify the FTP server information you specify. If you misconfigure any of the details, the FWSM fails to send log buffer data to the FTP server.

Examples

The following example shows how to specify an FTP server and enable the FWSM to write the contents of 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 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 syslog messages it contains.
logging buffered	Specifies the log buffer as an output destination, enabling event messages to be written to the log buffer as they occur.
logging buffer-size	Specifies log buffer size.
logging ftp-bufferwrap	Sends the log buffer contents to the specified FTP server when the log buffer wraps.
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 [*message_list* | *level*]

no logging history

Syntax Description

<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog 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.
<i>message_list</i>	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 FWSM does not log to SNMP servers 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging history** command lets you enable logging to an SNMP server and set the SNMP message level or event list. You must also configure the FWSM for SNMP.

Examples

The following example shows how to enable SNMP logging and specify that messages of severity levels 0, 1, 2, and 3 are sent to the SNMP server:

```
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
snmp-server	Specifies SNMP server details.

logging host

To define a syslog server as a log output destination, 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* *server_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**permit-hostdown**]

no logging host *interface_name* *server_ip*

Syntax Description

format emblem	(Optional) Enables EMBLEM format logging for the syslog server, which is available only for UDP messages.
host	Specifies a syslog server that will receive the messages that are sent from the FWSM.
<i>interface_name</i>	Interface on which the syslog server resides.
permit-hostdown	Allows new network access sessions for a TCP-based syslog server
<i>port</i>	The port that the syslog server listens to for messages. Valid port values for either protocol are 1025 through 65535.
<i>server_ip</i>	The IP address of the syslog server.
tcp	Specifies that the FWSM should use TCP to send messages to the syslog server.
udp	Specifies that the FWSM should use TCP to send messages to the syslog server.

Defaults

The default values are as follows:

- The default protocol is UDP.
- The default UDP port is 514.
- The default TCP port is 1470.

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
7.0(1)	This command was introduced.
7.2(2)	The permit-hostdown keyword was added.

Usage Guidelines

The **logging host** *ip_address* **format emblem** command lets you enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP syslog messages only. If you enable EMBLEM-format logging for a particular syslog server, then the messages are sent to that server in the EMBLEM format. If you also enable the **logging timestamp** keyword, messages sent to that server include a time stamp.

You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. For each server, you specify whether the server should receive messages using either the TCP or UDP protocol. You cannot specify a server to receive messages using both TCP and UDP.

To display *port* and *protocol* values that you entered previously, use the **show running-config logging** command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17. TCP ports work only with the FWSM syslog server. The *port* must be the same port on which the syslog server listens.

To continue to pass traffic through even when the TCP syslog server is down or unreachable, use the **permit-hostdown** keyword.

Examples

The following example shows how to send syslog messages of severity 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 host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging trap	Enables logging to syslog servers.

logging list

To create a list of message selection criteria to be used by other commands to specify which messages are sent to a particular output destination, 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** *message_class*] | **message** *start_id*[-*end_id*]}

no logging list *name*

Syntax Description

class <i>message_class</i>	(Optional) Specifies a class of syslog messages to be included in the list. See “ Usage Guidelines ” for a list of classes.
level <i>level</i>	Sets the maximum level for syslog messages. For example, if you set the level to 3, then the FWSM generates syslog messages for level 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. To look up the default level of a message, use the show logging command or see the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide</i> .
message <i>start_id</i> [- <i>end_id</i>]	Specifies a message ID or range of message IDs.
<i>name</i>	Specifies the message list name.

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
3.1(1)	This command was introduced.

Usage Guidelines

When you enable a log output destination, you can also specify which syslog messages should be sent to that destination. The message list enables you to specify one or more sets of criteria that the FWSM uses to select messages to be sent to a single output destination.

Criteria you can specify for message selection include severity level, message class, a message ID, or a range of message IDs.

You can specify more than one set of criteria for a single message list. To add a new set of criteria, reissue the command specifying the list name and the new criteria. The new criteria is appended to the existing message list.

Logging commands with which you can use message lists are as follows:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *message_class* include the following:

- **auth**—User authentication
- **bridge**—Transparent firewall
- **ca**—PKI certificate authority
- **config**—Command interface
- **e-mail**—E-mail proxy
- **ha**—Failover
- **ids**—Intrusion detection system
- **ip**—IP stack
- **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

The following example shows how to use the **logging list** command to create a new message list, append additional message selection criteria to the list, and specify that all messages matching the list criteria should be sent to the internal log buffer.

```
hostname(config)# logging list my-list 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 message selection criteria specified in this example are:

1. System log message IDs that fall in the range of 100100 to 100110
2. All syslog messages with critical level or higher (emergency, alert, or critical)
3. All VPN class syslog messages with warning level or higher (emergency, alert, critical, error, or warning)

If a syslog message satisfies any one of these conditions, it is logged to the internal log buffer.



Note

When you design list criteria, criteria can specify overlapping sets of messages. Syslog messages matching more than one criteria are logged normally.

Related Commands

Command	Description
show running-config logging	Displays the logging-related portion of the running configuration.

logging mail

To enable the FWSM to send syslog 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 syslog messages, use the **no** form of this command.

logging mail [*message_list* | *level*]

no logging mail [*message_list* | *level*]

Syntax Description	<i>level</i> Sets the maximum severity level for logging event messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity levels 3, 2, and 1. 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. <i>message_list</i> Specifies the list that identifies the messages to send to the e-mail recipient. For information about creating message 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		
Command Mode	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines	E-mailed syslog messages appear in the subject line of the e-mails sent.

Examples

The following example shows how to enable e-mail as an output destination, enabling syslog messages to be sent by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender's address.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according the example criteria, 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 from-address	Specifies the e-mail address that appears in the From: line of each e-mailed syslog message.
logging list	Creates a reusable list of message selection criteria.
logging recipient-address	Specifies the e-mail address to which e-mailed syslog messages are sent.
smtp-server	Configures an SMTP server.

logging message

To change the severity level of a syslog 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 FWSM from generating a particular syslog message, use the **no** form of the **logging message** command (without the **level** keyword) in global configuration mode. To let the FWSM generate a particular syslog message, use the **logging message** command (without the **level** keyword). These two purposes 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 severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog 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 syslog 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 <i>Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide</i>.

Defaults By default, all syslog 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:

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

You can use the **logging message** command for two purposes:

- To control whether a message is enabled or disabled.
- To change the severity level of a message.

You can use the **show logging** command to determine the severity level currently assigned to a message and whether the message is enabled.

Examples

The series of commands in the following example illustrates the use of the **logging message** command to enable and disable messages and change the severity level of 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.
show running-config logging	Displays the logging-related portion of the running configuration.

logging monitor

To enable the FWSM to display syslog messages in SSH and Telnet sessions, use the **logging monitor** command in global configuration mode. To disable the display of syslog messages in SSH and Telnet sessions, use the **no** form of this command.

logging monitor [*logging_list* | *level*]

no logging monitor

Syntax Description	<i>level</i> Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog messages for severity level 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.
	<i>logging_list</i> 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 FWSM does not display syslog messages in SSH and Telnet sessions 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
Global configuration	•	•	•	•	—

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines The **logging monitor** command enables syslog messages for all sessions in the current context; however, in each session, the **terminal** command controls whether syslog messages appear in that session.

Examples

The following example shows how to enable the display of syslog messages in console sessions. The use of the **errors** keyword indicates that messages of severity levels 0, 1, 2, and 3 should be shown 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 list	Creates a reusable list of message selection criteria to identify messages that should be sent to a particular output destination.
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 specify that the FWSM should allow new network access sessions for a TCP-based syslog server that is not operational, use the **logging permit-hostdown** command in global configuration mode. To specify that the FWSM should 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 FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM denies new network access sessions as a security measure if the FWSM 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 FWSM 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 host	Specifies a syslog server as an output destination.
logging trap	Enables logging to specified syslog servers.

logging queue

To specify how many syslog messages the FWSM can hold in its system log queue prior to processing them according to the current 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

<i>queue_size</i>	The number of syslog messages permitted in the queue used for storing syslog 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 FWSM might discard messages.

Examples

The following 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 zero, which means that the queue is set to the maximum of 8192. The syslog messages in the queue are processed by the FWSM in the manner dictated by the current logging configuration, such as sending syslog messages to e-mail recipients, saving buffer overflows to internal flash memory, and so forth.

The sample output of the **show logging queue** command shows that five messages are queued, 3513 messages was the largest number of messages in the queue at one time because the FWSM was last booted, and that one 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
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 syslog 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

<i>interval</i>	(Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for <i>interval</i> is 0 through 2147483647.
level <i>severity_level</i>	Applies the set rate limits on all syslog messages that belong to a certain severity level. All syslog messages at a specified severity level are rate-limited individually. The valid range for <i>severity_level</i> is 1 through 7.
message	Suppresses reporting of this syslog message.
<i>num</i>	Number of system messages that can be generated during the specified time interval. The valid range of values for <i>num</i> is 0 through 2147483647.
<i>syslog_id</i>	ID of the syslog message to be suppressed. The valid range of values for <i>syslog_id</i> 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
2.2(1)	This command was introduced in FWSM.

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 syslog message generation, you can enter a specific message ID. The following example shows how to limit the rate of syslog message generation using a specific message ID and time interval:

```
fwsm(config)# logging rate-limit 100 600 message 302020
```

This example suppresses syslog 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 syslog message generation, you can enter a specific severity level. The following example shows how to limit the rate of syslog message generation using a specific severity level and time interval.

```
fwsm(config)# logging rate-limit 1000 600 level 6
```

This example suppresses all syslog messages under severity level 6 to the specified rate-limit of 1000 in the specified time interval of 600 seconds. Each syslog 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 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 syslog messages e-mailed by the FWSM, 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 five recipient addresses. You can choose to specify a different message level for each recipient address. The message level specified with this command takes precedence over the message level specified by the **logging mail** command.

logging recipient-address *email_address* [**level** *level*]

no logging recipient-address *email_address* [**level** *level*]

Syntax Description

<i>email_address</i>	Specifies recipient e-mail address when sending syslog messages by e-mail.
level	Indicates that a logging level follows.
<i>level</i>	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the FWSM generates syslog 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 syslog messages due to 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 severity level of 3, the FWSM sends all messages to the recipient, including those of severity 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	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Sending syslog messages by e-mail is enabled by the **logging mail** command.

You can configure up to five e-mail addresses to receive syslog messages from the FWSM. Enter a new command for each recipient you want to specify. Each recipient can have a different logging level than the others. This is useful when you want more urgent messages to go to a larger number of recipients than less urgent messages.

Examples

The following example shows how to set up the FWSM to send a limited number of syslog messages by e-mail. The example commands are based on the following example criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the address of the sender.
- Send messages to admin@example.com.
- Send messages using SMTP the primary servers pri-smtp-host and secondary server sec-smtp-host.

To enable the FWSM to e-mail system messages according to the example criteria, 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 to all specified output locations.
logging from-address	Specifies the e-mail address that appears in the From: line of each e-mailed syslog message.
logging mail	Enables the FWSM to send syslog messages by e-mail and specifies 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 current contents of the log buffer to internal flash memory, use the **logging savelog** command in privileged EXEC mode.

logging savelog [*savefile*]

Syntax Description

<i>savefile</i>	(Optional) File name to use for saving log data to internal flash memory. If you do not specify a file name, the FWSM saves the file using a default time-stamp format, as follows: <i>LOG-YYYY-MM-DD-HHMMSS.TXT</i> where <i>YYYY</i> is the year, <i>MM</i> is the month, <i>DD</i> is the day of the month, and <i>HHMMSS</i> 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 preceding table.

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
3.1(1)	This command was introduced.

Usage Guidelines

Before you can save the contents of the log buffer to internal flash memory, you must enable logging to the buffer; if logging to the buffer is not enabled, the FWSM does not save syslog messages to the buffer, and therefore the buffer is empty. 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

The following example enables the log buffer as an output destination, exits global configuration mode, and saves the log buffer to internal flash memory, using the file name latest-logfile.txt:

```
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 syslog 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 internal log buffer.
show logging	Displays contents of the internal log buffer and the enabled logging options.

logging standby

To enable the failover standby FWSM to send the syslog messages of this FWSM to configured logging destinations, use the **logging standby** command in global configuration mode. To disable system log 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:

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

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines You can enable **logging standby** to ensure that the syslog messages of the failover standby FWSM stay synchronized if failover occurs.



Note

Using the **logging standby** command creates twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

Examples The following example enables the FWSM to send syslog messages to the failover standby FWSM. 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 host	Defines a syslog server.
show running-config logging	Displays the logging-related portion of the running configuration.

logging timestamp

To specify that syslog 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 syslog messages, use the **no** form of this command.

logging timestamp

no logging timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

The FWSM does not include the date and time in syslog messages 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging timestamp** command causes the FWSM to include a timestamp in all syslog messages.

Examples

The following example enables the inclusion of timestamp information in all syslog messages:

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging to all specified output destinations.
show logging	Displays contents of the internal log buffer and the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

login

To log in to privileged EXEC mode using the local user database (see the **username** command) or to change usernames, 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 only use the **login** command in user EXEC mode. If you are already in privileged EXEC mode, you need to enter the **disable** command to go back to user EXEC mode where you can enter the **login** command.

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.

When you use the **login** command in the system execution space, the FWSM uses the username database in the admin context. You cannot enter the **username** command directly in the system execution space.



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.

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 of 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
User EXEC	•	•	•	•	•

Release	Modification
1.1(1)	This command was introduced.

Command History

Usage Guidelines The **logout** command lets you log out of the FWSM. You can use the **exit** or **quit** commands to go back to user EXEC mode.

Examples The following example shows how to log out of the FWSM:

```
hostname> logout
```

Command	Description
login	Initiates the log-in prompt.
exit	Exits an access mode.
quit	Exits configuration or privileged mode.

Related Commands



CHAPTER

20

mac-address-table aging-time through multicast-routing Commands

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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.

mac-address-table static *interface_name* *mac_address*

no mac-address-table static *interface_name* *mac_address*

Syntax Description

<i>interface_name</i>	Sets the source interface.
<i>mac_address</i>	Sets 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

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 FWSM drops the traffic and generates a system message.

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.

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

Syntax Description

<i>interface_name</i>	Sets 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, each interface automatically learns the MAC addresses of entering traffic, and the FWSM adds corresponding entries to the MAC address table. You can disable MAC address learning if desired.

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.

Command	Description
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.
<i>id</i>	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.
<i>mac</i>	Specifies the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn
<i>macmask</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 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.

management-access

To allow management access to an interface other than the one you entered the FWSM from, use the **management-access** command in global configuration mode. To disable this access, use the **no** form of this command.

management-access *mgmt_if*

no management-access *mgmt_if*

Syntax Description

<i>mgmt_if</i>	Specifies the name of the management interface you want to access when entering the FWSM from another interface.

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
3.1(1)	This command was introduced.

Usage Guidelines

This command allows you to connect to an interface other than the one you entered the FWSM from. For example, if you enter the FWSM 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 define only one management interface.

The **management-access** command is supported for the following through an IPSec VPN tunnel only:

- SNMP polls to the management interface
- HTTPS requests to the management interface
- ASDM access to the management interface
- Telnet access to the management interface
- SSH access to the management interface
- Ping to the management interface
- Syslog polls to the management interface
- NTP requests 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 interface for management access of the FWSM.
show management-access	Displays the name of the interface configured for management access.

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.

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
Interface configuration	•	—	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enables management-only mode on a subinterface:

```
hostname(config)# interface gigabitethernet2.1
hostname(config-subif)# management-only
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

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. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. This mask action is available in an inspection policy map for application traffic; however, not all applications allow this action. For example, you can use **mask** command for the HTTP application inspection to mask text in a message header before allowing the traffic through the FWSM. To disable this action, use the **no** form of this command.

mask [**log**]

no mask [**log**]

Syntax Description

log (Optional) 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:

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

Command History

Release	Modification
4.0(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 http http_policy_map** command where *http_policy_map* is the name of the inspection policy map.

Examples

The following example masks the HTTP response if the content-type field does not match the accept field in the corresponding HTTP request message before allowing the traffic through the FWSM:

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap-c)# match req-resp content-type mismatch
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-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:

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

Command History

Release	Modification
3.1(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 FWSM 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)# exit
```

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.
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:

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

Command History

Release	Modification
3.1(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 FWSM 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:

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

Command History

Release	Modification
3.1(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

The following 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
```

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 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.
<i>bytes</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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:

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

Command History

Release	Modification
4.0(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:

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

Command History

Release	Modification
4.0(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 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 <i>verb</i>	Specifies the ESMTP command verb.
line length gt <i>bytes</i>	Specifies the length of a line.
RCPT count gt <i>recipients_number</i>	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:

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

Command History

Release	Modification
4.0(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 content

To configure a match condition on the SIP content header, use the **match content** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **content** [**regex** *regex*]

no match [**not**] **match** [**not**] **content** [**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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the content in a SIP inspection class map:

```
hostname(config-cmap)# match content regex sample
```

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:

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

Command History

Release	Modification
3.1(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
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
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
xmcp	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
```

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 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:

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

Command History

Release	Modification
4.0(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 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:

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

Command History

Release	Modification
4.0(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 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 condition, 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

<i>regex_name</i>	Specifies a regular expression.
class <i>regex_class_name</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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 interface

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. To remove the match interface entry, use the **no** form of this command.

match interface *interface-name...*

no match interface *interface-name...*

Syntax Description

interface-name Name of the interface as specified by the **nameif** command. You can specify multiple interface names.

Defaults

No match interfaces are defined.

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
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the interface-type interface-number arguments.

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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 give the **match** commands in any order. All **match** commands must “pass” to cause the route to be redistributed according to the set actions that are given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria. If there is more than one interface specified in the **match** command, then the **no match interface interface-name** can be used to remove a single interface.

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. If you want to modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows that the routes with their next hop outside is distributed:

```
hostname(config)# route-map name  
hostname(config-route-map)# match interface outside
```

Related Commands

Command	Description
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 ip route-source	Redistributes routes that have been advertised by routers and access servers at the address that is specified by the access lists.
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 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:

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

Command History

Release	Modification
4.0(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 Specifies an ACL by name. You can specify multiple ACLs.

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
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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

<i>acl</i>	Name of an ACL. You can specify multiple ACLs.
prefix-list <i>prefix_list</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 let you 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# 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 access lists, 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...* | **prefix-list** *prefix_list*}

Syntax Description

<i>acl</i>	Name of an ACL. You can specify multiple ACLs.
<i>prefix_list</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 let you 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 access lists `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 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 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 condition, 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

<i>regex_name</i>	Specifies a regular expression.
class <i>regex_class_name</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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.

 match message-path

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 metric

To redistribute routes with the metric specified, use the **match metric** command in route-map configuration mode. To remove the entry, use the **no** form of this command.

match metric *number*

no match metric *number*

Syntax Description

number Route metric; valid values are from 0 to 4294967295.

Defaults

No filtering on a metric value.

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
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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. The **match** commands can be given 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** 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.

Examples

The following example shows how to redistribute routes with the metric 5:

```
hostname(config)# route-map name
hostname(config-route-map)# match metric 5
```

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.
	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 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 <i>type</i>	Specifies to match on the encoding type.
filename length <i>gt bytes</i>	Specifies to match on the filename length.
filetype <i>regex</i>	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:

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

Command History

Release	Modification
4.0(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 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 <i>port</i>	Specifies a single port name or number.
range <i>beg_port</i> <i>end_port</i>	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:

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

Command History

Release	Modification
3.1(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 port** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** 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 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 condition, use the **no** form of this command.

match [**not**] **request-method** *method_type*

no match [**not**] **request-method** *method_type*

Syntax Description

<i>method_type</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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, response

To perform matches on HTTP headers for HTTP inspection, use the **match request, response** command in policy-map configuration mode. To not match on HTTP headers, use the **no** form of this command.

```
match [not] { request | response } header { header_name | content-type | transfer-encoding |
length gt bytes | count number } { built_in_regex | regex class class_map_name | regex
regex_name | length gt bytes | count number }
```

```
no match [not] { request | response } header { header_name | content-type | transfer-encoding
| length gt bytes | count number } { built_in_regex | regex class class_map_name | regex
regex_name | length gt bytes | count number }
```

Syntax Description

header	Specifies the of the HTTP message.
<i>header_name</i>	Specifies the name of the HTTP header to match.
content-type	Specifies to match the content type in the response to the accept types in the request.
transfer-encoding	
length gt bytes	Specifies to match on the length of the HTTP header message.
count number	
<i>built_in_regex</i>	Specifies the built-in regex for content type, method, or transfer encoding.
regex class	Specifies the name of the class map of regex type.
<i>class_map_name</i>	
<i>regex regex_name</i>	Specifies the name of the regular expression configured using the regex command.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy- map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Total Header Length Check

The following command performs a check to determine if the entire header portion of the HTTP message is greater than *bytes*:

```
[no] match [not] { request | response } header length gt <bytes>
```

Count of All Header Fields Check

The following command performs a check to determine if the number of header fields in the HTTP message is greater than *number*:

```
hostname(config-pmap)# [no] match [not] { request | response } header count number
```

Total Header Regex Check

The following command performs a regex scan of the entire header of the HTTP message. This can be useful for checking for non-ASCII characters.

```
hostname(config-pmap)# [no] match [not] { request | response } header regex { class  
class_map_name | regex_name }
```

Specified Header Field Length Check

The following command performs a length check of an individual header field to ensure that it is less than *bytes* characters long:

```
hostname(config-pmap)# [no] match [not] { request | response } header { header_name |  
content-type | transfer-encoding } length gt bytes
```



Note

Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

```
hostname(config)# regex foo [Ff][0o][0o]  
hostname(config)# policy-map  
hostname(config-pmap)# match request header foo length gt 99
```

Specified Header Field Count Check

The following command will count the instances of the specified field and perform a check to ensure that it occurs less than *<number>* of times.

```
hostname(config-pmap)# [no] match [not] { request | response } header { header_name |  
content-type | transfer-encoding } count number
```



Note

Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

```
hostname(config)# regex foo [Ff][0o][0o]  
hostname(config)# policy-map  
hostname(config-pmap)# match request header foo count 3
```

Specified Header Field Regex Value Check

The following command will attempt to match the specified regex or regex class against value of the specified field:

```
hostname(config-pmap)# [no] match [not] { request | response } header { header_name |  
content-type | transfer-encoding } regex { class class_map_name | regex_name }
```



Note

Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

```
hostname(config)# regex foo [Ff][0o][0o]
```

```
hostname(config)# regex bar [Bb][Aa][Rr]
hostname(config)# policy-map
hostname(config-pmap)# match request header foo regex bar
```

Content-type Header Check

In addition to the length, count and regex checks described above, the user can perform various special checks on the content type field:

- The user can match the mime-type in the header's value against a set of built-in keywords for the known mime-types.
- The user can also specify that the mime-type must one of the built-ins by using the “unknown” keyword.
- The user can also cause content-type verification to be done by specifying the “violation” keyword. Content-type verification will check the “magic number” in the body of the HTTP message against the mime-type's magic number to ensure that some other type is not being smuggled.

The following types are built-in. Many have magic numbers associated with them and can be verified. The **count**, **length**, and **regex** keywords operate the same as for the other fields as described above.

```
hostname(config-pmap)# match { request | response } header content-type ?
```

Content type	Match on
application/msword	Match on 'application/msword'
application/octet-stream	Match on 'application/octet-stream'
application/pdf	Match on 'application/pdf'
application/postscript	Match on 'application/postscript'
application/vnd.ms-excel	Match on 'application/vnd.ms-excel'
application/vnd.ms-powerpoint	Match on 'application/vnd.ms-powerpoint'
application/x-gzip	Match on 'application/x-gzip'
application/x-java-archive	Match on 'application/x-java-archive'
application/x-java-vm	Match on 'application/x-java-vm'
application/x-msn-messenger	Match on 'application/x-msn-messenger'
application/zip	Match on 'application/zip'
audio/basic	Match on 'audio/basic'
audio/midi	Match on 'audio/midi'
audio/mpeg	Match on 'audio/mpeg'
audio/x-adpcm	Match on 'audio/x-adpcm'
audio/x-aiff	Match on 'audio/x-aiff'
audio/x-ogg	Match on 'audio/x-ogg'
audio/x-wav	Match on 'audio/x-wav'
count	Specify that the match should count the number of instances of this header
image/gif	Match on 'image/gif'
image/jpeg	Match on 'image/jpeg'
image/mpeg	Match on 'image/mpeg'

Content type	Match on
image/tiff	Match on 'image/tiff
image/x-3ds	Match on 'image/x-3ds
image/x-bitmap	Match on 'image/x-bitmap
image/x-niff	Match on 'image/x-niff'
image/x-png	Match on 'image/x-png
image/x-portable-bitmap	Match on 'image/x-portable-bitmap
image/x-portable-graymap	Match on 'image/x-portable-graymap
image/x-xpm	Match on 'image/x-xpm
length	Specify that the match is a length check
regex	Specify a regex or regex class
text/css	Match on 'text/css
text/html	Match on 'text/html
text/plain	Match on 'text/plain
text/richtext	Match on 'text/richtext'
text/sgml	Match on 'text/sgml
text/xmcd	Match on 'text/xmcd'
text/xml	Match on 'text/xml
unknown	Specify that the mime-type must match a built-in 'known' mime-type
video/flc	Match on 'video/flc
video/mpeg	Match on 'video/mpeg
video/quicktime	Match on 'video/quicktime
video/sgi	Match on 'video/sgi
video/x-fli	Match on 'video/x-fli
violation	Specify that the 'magic number' in the body must correspond to the mime-type in the content-type header field

Transfer-Encoding Header Check

In addition to the length, count and regex checks described above, the user can perform various special checks on the transfer-encoding field:

- The user can match the transfer encoding in the header's value against a set of built-in keywords for the known transfer-encodings.
- The user can also specify that the transfer-encoding must be populated by using the “empty” keyword.
- The following types are built-in. Many of them have magic numbers associated with them and can be verified. The “count”, “length” and “regex” options operate the same as for the other fields as described above.

```
hostname(config-pmap) # match { request | response } header transfer-encoding ?
```

See the following **mpf-class-map** mode commands and options:

Command	Match on
chunked	Match on 'chunked'
compress	Match on 'compress'
count	Specify that the match should count the number of instances of this header
deflate	Match on 'deflate'
empty	Match an empty transfer-encoding field
gzip	Match on 'gzip'
identity	Match on 'identity'
length	Specify that the match is a length check
regex	Specify a regex or regex class

Examples

The following example shows the use of the **match request, response** command to performs a regex scan of the entire header of the HTTP message:

```
hostname(config-pmap) # match request header regex class classmap1 regex1
```

Related Commands

Command	Description
policy map type inspect	When using the Modular Policy Framework, defines special actions for inspection application traffic.
inspect http	Inspects HTTP traffic.

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

external	Match OSPF external routes (type 1 or type 2).
internal	Match OSPF intra-area and interarea routes.
local	Match a locally generated route.
nssa-external	Match OSPF NSSA external route (type 1 or type 2).
type-1	(Optional) Match only type 1 routes.
type-2	(Optional) Match only type 2 routes.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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.

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 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 <i>bytes</i>	Specifies to match on the sender e-mail address length.
regex <i>regex</i>	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:

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

Command History

Release	Modification
4.0(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 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 condition, 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

<i>regex_name</i>	Specifies a regular expression.
class <i>regex_class_name</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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 registrar 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 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 condition, 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 <i>gt_bytes</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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.

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 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
AAA-server group	•	•	•	•	—

Command History

Release	Modification
3.1(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
```

Related Commands

Command	Description
aaa-server <i>server-tag</i> protocol <i>protocol</i>	Enters AAA server group configuration mode so that 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:

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

Command History

Release	Modification
4.0(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:

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

After enabling the **max-header-length** command, the FWSM only allows messages having an HTTP header within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the FWSM 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 FWSM 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)# exit
```

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-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:

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

After enabling the **max-uri-length** command, the FWSM only allows messages having a URI within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the FWSM 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 FWSM 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)# exit
```

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

<i>country_code</i>	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.
<i>network_code</i>	A two or three-digit value identifying the network code.

Defaults

By default, the FWSM does not check for valid MCC/MNC combinations.

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
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(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 FWSM does not check the validity of MNC and MCC combinations; therefore, 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 gtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
```

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.

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the FWSM, 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 FWSM 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)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passwd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0
```

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.

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

<i>endPC</i>	Specifies the end address range of the memory block.
<i>startPC</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
3.1(1)	Support for 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 FWSM 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 FWSM.
show memory-caller address	Displays the address ranges configured on the FWSM.

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:

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

Command History	Release	Modification
	3.1(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 FWSM 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
```

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 20-1 describes the significant portion of the output.

Table 20-1 *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 20-1 *Illegal Memory Usage Output Description*

Field	Description
allocated by/freed by	Instruction addresses where the last malloc/calloc/realloc and free calls were 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 enable

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:

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

Release	Modification
3.1(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 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

<i>peak_value</i>	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:

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

Command History

Release	Modification
3.1(1)	Support for 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 FWSM 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 FWSM.

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.
<i>endPC</i>	Specifies the end text range of the memory block.
<i>resolution</i>	Specifies the resolution of tracing for the source text region.
<i>startPC</i>	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:

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

Command History

Release	Modification
3.1(1)	Support for 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 FWSM 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 FWSM.
show memory-caller address	Displays the address ranges configured on the FWSM.

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.
<i>max_bytes</i>	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.
<i>min_bytes</i>	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		
	Routed	Transparent	Single	Multiple Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(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 gtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
```

Related Commands

message-length

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:

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

Command History

Release	Modification
3.1(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 Vlan55
hostname(config-if)# no mfib forwarding
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing.
pim	Enables PIM on an interface.

mgcp-map

To identify a specific map for defining the parameters for MGCP inspection, use the **mgcp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

mgcp-map *map_name*

no mgcp-map *map_name*

Syntax Description

map_name The name of the MGCP map. The maximum number of characters is 64.

Defaults

The default for the MGCP command queue is 200.

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
3.1(1)	This command was introduced.

Usage Guidelines

Use the **mgcp-map** command to identify a specific map to use for defining the parameters for MGCP inspection. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. After defining the MGCP map, you use the **inspect mgcp** command to enable the map. You use Modular Policy Framework to apply the **inspect** command to a defined class of traffic and to apply the policy to a specific interface. The following are the commands available in MGCP map configuration mode.

- **call-agent**—Specifies a group of call agents.
- **command-queue**—Specifies the maximum number of MGCP commands that can be queued.
- **gateway**—Specifies the group of call agents that are managing a particular gateway.
- **no**—Negates a command or sets a parameter to its default value.

Examples

The following example shows how to use the **mgcp-map** command to identify a specific map (mgcp-policy) to use for defining the parameters for MGCP inspection.

```
hostname(config)# mgcp-map mgcp-policy
hostname(config-mgcp-policy)#
```

The following example shows how to identify MGCP traffic, define a MGCP map, define a policy, and apply the policy to the outside interface. You enable the MGCP inspection engine as shown in the following example, which creates a class map to match MGCP traffic on the default port (2427). The service policy is then applied to the outside interface.

```
hostname(config)# class-map mgcp-port
hostname(config-cmap)# match port tcp eq 2427
hostname(config-cmap)# exit
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
hostname(config-mgcp-map)# command-queue 150
hostname(config)# policy-map mgcp_policy
hostname(config-pmap)# class mgcp-port
hostname(config-pmap-c)# inspect mgcp mgcp_inbound
hostname(config-pmap-c)# exit
hostname(config)# service-policy mgcp_policy interface outside
```

This 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
debug mgcp	Enables the display of debug information for MGCP.
show mgcp	Displays MGCP configuration and session information.
timeout	Configures the idle timeouts related to MGCP.

mkdir

To create a new directory, use the **mkdir** command in privileged EXEC mode.

mkdir [/noconfirm] [flash:]*path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
<i>path</i>	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:

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

Command History

Release	Modification
3.1(1)	Support for 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 FWSM 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 FWSM 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the FWSM 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 FWSM. 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 FWSM 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 FWSM 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 FWSM; 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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* 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 logical interfaces 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The number of interfaces that can be monitored for the FWSM is 250. Hello messages are exchanged during every interface poll frequency time period between the FWSM 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	Removes the monitor-interface commands from the running configuration.
	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 in privileged EXEC mode.

more {/ascii | /binary | /ebcdic | 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.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
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:

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

Command History	Release	Modification
	2.2(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.

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* | *rpf_neighbor*} [**dense** *output_if_name*] [*distance*]

no mroute *src smask* {*in_if_name* | *rpf_neighbor*} [**dense** *output_if_name*] [*distance*]

Syntax Description

dense <i>output_if_name</i>	(Optional) The interface name for dense mode output. The dense <i>output_if_name</i> keyword and argument pair is only supported for SMR stub multicast routing (igmp forwarding).
<i>distance</i>	(Optional) The administrative distance of the route. Routes with lower distances have preference. The default is 0.
<i>in_if_name</i>	Specifies the incoming interface name for the mroute.
<i>rpf_neighbor</i>	Specifies the RPF neighbor for the security appliance.
<i>smask</i>	Specifies the multicast source network address mask.
<i>src</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command lets you statically configure where multicast sources are located. The FWSM 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.



Note

You can specify the interface name or the RPF neighbor using this command, but not at the same time.

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
show running-config mroute	Displays the mroute commands in the configuration.

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

<i>bytes</i>	Number of bytes in the MTU; valid values are from 64 to 65,535 bytes.
<i>interface_name</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM 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-routing

To enable IP multicast routing on the FWSM, 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:

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

Command History

Release	Modification
3.1(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 20-2](#) 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 20-2 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 FWSM:

```
hostname(config)# multicast-routing
```

Related Commands

Command	Description
igmp	Enables IGMP on an interface.
pim	Enables PIM on an interface.



CHAPTER

21

name through ospf transmit-delay Commands

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*

no name *ip_address [name]*

Syntax Description

<i>ip_address</i>	Specifies an IP address of the host that is named.
<i>name</i>	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 <i>name</i> must be 63 characters or less. Also, the <i>name</i> cannot start with a number.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM instead of the interface type and ID (such as gigabitethernet1), 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

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 gigabitethernet1
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
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.

names

To enable IP address to the name conversions that you can configured with the **name** command, use the **names** command in global configuration mode. To disable address to name conversion, use the **no** form of this 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

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 <i>access_list_name</i>	Identifies the real addresses and destination addresses using an extended access list, also known as policy NAT. Create the access list using the access-list command. This access list should include only permit ACEs. 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.
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 a real interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from a real 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.
<i>emb_limit</i>	(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 FWSM 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.

<i>mask</i>	(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.
<i>nat_id</i>	Specifies an integer for the NAT ID. This ID is referenced by the global command to associate a global pool with the <i>real_ip</i>. 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.
norandomseq	(Optional) Disables TCP ISN randomization protection. TCP initial sequence number randomization can be disabled if another in-line firewall is also randomizing the initial sequence numbers, because there is no need for both firewalls to be performing this action. However, leaving ISN randomization enabled on both firewalls does not affect the traffic. 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 the outbound direction. If the connection is between two interfaces with the same security level, then the ISN will be randomized in the SYN in both 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. The norandomseq keyword does not apply to outside NAT. The firewall randomizes only the ISN that is generated by the host/server on the higher security interface. If you set norandomseq for outside NAT, the norandomseq keyword is ignored.
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.
<i>real_ifc</i>	Specifies the name of the interface connected to the real IP address network.
<i>real_ip</i>	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 <i>tcp_max_conns</i>	(Optional) Specifies the maximum number of simultaneous TCP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the timeout conn command.)
udp <i>udp_max_conns</i>	(Optional) Specifies the maximum number of simultaneous UDP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the timeout conn command.)

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
2.3(1)	This command was modified to allow connection settings for outside NAT.
3.2.(1)	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.

The FWSM 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 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 FWSM 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 FWSM rejects any attempt to connect to a real host address directly. See the **static** command for reliable access to hosts.

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.

PAT translates multiple real addresses to a single mapped IP address. Specifically, the FWSM 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 FWSM 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.

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.

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, and so on.), the FWSM 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.

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 FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

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-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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.
3.2.(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.

By default, NAT control is disabled, so you do not need to perform NAT on any networks unless you choose to perform NAT.

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.



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.

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.

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:

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

Command History

Release	Modification
3.1(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 <i>name</i>	The interface name, as specified by the nameif command, through which the neighbor can be reached.
<i>ip_address</i>	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:

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

Command History

Release	Modification
4.0(1)	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
```

neighbor (EIGRP)

```
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.

neighbor password

To specify MD5 authentication for the specified BGP neighbor, use the **neighbor password** command in router configuration mode. To remove the password, use the **no** form of this command.

neighbor *ip-addr* **password** [*mode*] *password*

no neighbor *ip-addr* **password** [*mode*] *string*

Syntax Description

<i>ip-addr</i>	The IP address of the BGP neighbor.
<i>mode</i>	A number from 0 to 7. DO NOT USE THIS OPTIONAL ARGUMENT. No one knows what it does and it could break the authentication.
<i>password</i>	A case-sensitive password of up to 25 characters. The <i>password</i> can contain alphanumeric characters and the following symbols: ` ~ ! @ # \$ % ^ & * ( ) - _ = +   \ } ] { [ " ` ; / > < . , ? The <i>password</i> cannot contain spaces.

Defaults

There are no BGP neighbors defined.

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 ¹	System
Router configuration	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You can configure MD5 authentication between two BGP peers. Each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example enables the authentication of BGP messages exchanged with the BGP neighbor. The neighbor device must be configured with the same password.

```
hostname(config)# router bgp 800
hostname(config-router)# bgp router-id 192.168.1.1
hostname(config-router)# neighbor 10.1.1.1 remote-as 800
hostname(config-router)# neighbor 10.1.1.1 password bQ2$f78t
hostname(config-router)# network 192.168.1.0 mask 255.255.255.0
hostname(config-router)# network 10.1.1.0 mask 255.255.255.0
```

Related Commands

Command	Description
neighbor remote-as	Defines a BGP neighbor.
router bgp	Creates a BGP routing process and enters router configuration mode for that process.
show running-config router	Displays the router commands in the running configuration.

neighbor remote-as

To specify the BGP neighbor, use the **neighbor remote-as** command in router configuration mode. To remove the neighbor, use the **no** form of this command.

neighbor *ip-addr* **remote-as** *as-number*

no neighbor *ip-addr* **remote-as** *as-number*

Syntax Description

<i>as-number</i>	Autonomous system to which the neighbor belongs.
<i>ip-addr</i>	The IP address of BGP neighbor.

Defaults

There are no BGP neighbors defined.

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 ¹	System
Router configuration	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

The FWSM must be in the same AS as the defined neighbor.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example assigns the FWSM an AS number of 800. The BGP neighbor at 10.1.1.1 is also part of AS 800.

```
hostname(config)# router bgp 800
hostname(config-router)# bgp router-id 192.168.1.1
hostname(config-router)# neighbor 10.1.1.1 remote-as 800
hostname(config-router)# neighbor 10.1.1.1 password bQ2$F78t
hostname(config-router)# network 192.168.1.0 mask 255.255.255.0
hostname(config-router)# network 10.1.1.0 mask 255.255.255.0
```

■ neighbor remote-as

Related Commands	Command	Description
	neighbor password	Defines the password used for MD5 authentication of BGP messages exchanged with the BGP neighbor.
	router bgp	Creates a BGP routing process and enters router configuration mode for that process.
	show running-config router	Displays the router commands in the running configuration.

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:

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

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 FWSM. PAT does not apply. Therefore, devices behind the FWSM 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
3.1(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 the networks that are advertised by the BGP routing process, use the **network** command in router configuration mode. To remove the password, use the **no** form of this command.

```
network ip-addr mask mask

no network ip-addr mask mask
```

Syntax Description

<i>ip-addr</i>	The IP address of the network to advertise.
mask mask	The network mask applied to the <i>ip-addr</i> argument.

Defaults

There are no networks advertised.

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 ¹	System
Router configuration	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

The network command determine which static or directly connected networks are advertised to the defined BGP neighbor. You can have a maximum of 200 network commands configured on the FWSM.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example causes the 192.168.1.0 and 10.1.1.0 networks to be included in BGP updates sent by the FWSM to the BGP neighbor:

```
hostname(config)# router bgp 800
hostname(config-router)# bgp router-id 192.168.1.1
hostname(config-router)# neighbor 10.1.1.1 remote-as 800
hostname(config-router)# neighbor 10.1.1.1 password bQ2$f78t
hostname(config-router)# network 192.168.1.0 mask 255.255.255.0
hostname(config-router)# network 10.1.1.0 mask 255.255.255.0
```

Related Commands	Command	Description
	neighbor	Specifies the BGP neighbor.
	router bgp	Creates a BGP routing process and enters router configuration mode for that process.
	show running-config router	Displays the router commands in the running 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	<i>ip_addr</i>	The IP address of a directly connected network. The interface connected to the specified network will participate in the EIGRP routing process.
	<i>mask</i>	(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:

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

Command History	Release	Modification
	4.0(1)	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 FWSM then establishes neighbors through the matched interfaces. There is no limit to the number of **network** commands that can be configured on the FWSM.

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 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

<i>addr</i>	IP address.
area <i>area_id</i>	Specifies the area that is to be associated with the OSPF address range. The <i>area_id</i> can be specified in either IP address format or in decimal format. When specified in decimal format, valid values range from 0 to 4294967295.
<i>mask</i>	The network mask.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM.

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 hostname is not already defined using the name command).
host_name	Hostname (if the hostname is defined using the name command).
net_addr	Network address; used with <i>netmask</i> to define a subnet object.
netmask	Netmask; used with <i>net_addr</i> 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 mode. To remove this specification, use the **no** form of this command:

nt-auth-domain-controller *hostname*

no nt-auth-domain-controller

Syntax Description

hostname 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is valid only for NT authentication 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(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
```

Related Commands

Command	Description
aaa-server	Enters AAA server host configuration mode so that 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.

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.
<i>obj_grp_id</i>	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	Defines a group of TCP/UDP port specifications such as “eq smtp” and “range 2000 2010.” 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
1.1(1)	This command was introduced.

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 FWSM 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 FWSM 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
<i>protocol</i>	object-group <i>protocol</i>
<i>host and subnet</i>	object-group <i>network</i>
<i>service</i>	object-group <i>service</i>
<i>icmp_type</i>	object-group <i>icmp_type</i>

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 FWSM.

However, when you enter the **object-group** command, the prompt appears as follows:

```
hostname(config-type)#
```

where *hostname* is the name of the FWSM, 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 FWSM 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.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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

<i>password</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

Examples

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

<i>interface_cost</i>	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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 lets you 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
<code>show running-config interface</code>	Displays the configuration of the specified interface.

ospf database-filter all out

To filter out all outgoing LSAs to an OSPF interface during synchronization and flooding, use the **ospf database-filter all out** 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

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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ospf database-filter all out** 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ospf dead-interval** command lets you set the dead interval before neighbors 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 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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

<i>key-id</i>	Enables MD5 authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
md5 <i>key</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ospf message-digest-key** command lets you enable MD5 authentication. The **no** form of the command removes an MD5 key. The *key_id* argument is a numerical identifier from 1 to 255 for the authentication key. The *key* argument 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
3.1(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 resend 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 retransmit-delay 3
hostname(config-if)#
```

Related Commands

Command	Description
show ospf interface	Displays OSPF-related interface information.



CHAPTER

22

pager through pwd Commands

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:

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

Command History

Release	Modification
3.1(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 or session to the system execution space, 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.

If there are two or more concurrent Telnet or ssh sessions, and one of the sessions is at the “---more---” (more) prompt, the other sessions cannot do anything until the more prompt is dismissed. To avoid the more prompt altogether, enter the **pager lines 0** command.

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 messages 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:

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

Command History	Release	Modification
	4.0(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.

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 reenale 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.
<i>if_name</i>	(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:

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

Command History

Release	Modification
4.0(1)	This command was introduced.

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 FWSM 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.
<i>password</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM:

```
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

<i>string</i>	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:

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

Command History

Release	Modification
3.1(1)	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 FWSM.

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 zzxyyy
hostname(ca-trustpoint)#
```

Related Commands

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

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:

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

Command History

Release	Modification
3.1(1)	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 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

<i>option</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all 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-ipsec)# peer-id-validate req
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the configuration for the indicated tunnel group or for all tunnel groups.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

perfmon

To enable the FWSM to capture performance information on a periodic basis, use the **perfmon verbose** command in privileged EXEC mode. To disable performance information output, use the **perfmon quiet** command. To view the performance information that was captured, use the **show console-output** command.

perfmon { verbose | quiet }

Syntax Description

verbose	Captures performance information.
quiet	Disables performance monitoring.

Defaults

The default interval is 120 seconds. See the **perfmon interval** command to set the interval.

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
1.1(1)	This command was introduced.

Usage Guidelines

Output from the **perfmon** command displays in the Telnet or SSH session terminal window and is directed to the console only if the session terminates. If a terminated session is re-established, the command output re-appears in the session window.

Examples

This example shows how to capture the performance monitor statistics every 30 seconds:

```
hostname# perfmon interval 30
hostname# perfmon verbose
hostname# show console-output
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

Related Commands

Command	Description
perfmon settings	Shows the performance monitoring settings.
perfmon interval	Sets the performance monitoring capture interval.
show console-output	Shows the console buffer.
show perfmon	Displays performance information immediately.

perfmon interval

To set the interval in seconds to capture performance information, use the **perfmon interval** command in privileged EXEC mode.

perfmon interval *seconds*

Syntax Description

seconds Specifies the number of seconds before the performance display is refreshed.

Defaults

The *seconds* is 120 seconds.

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
1.1(1)	This command was introduced.

Usage Guidelines

To enable performance monitoring, enter the **perfmon verbose** command. To disable it, enter the **perfmon quiet** command. Output from the **perfmon** command displays in the Telnet or SSH session terminal window and is directed to the console only if the session terminates. If a terminated session is re-established, the command output appears in the new session window.

Examples

This example shows how to capture the performance monitor statistics every 30 seconds:

```
hostname# perfmon interval 30
hostname# perfmon verbose
```

Related Commands

Command	Description
perfmon	Enables the FWSM to capture performance monitoring information.
perfmon settings	Shows the performance monitoring settings.
show console-output	Shows the console buffer.
show perfmon	Displays performance information.

perfmon settings

To view the performance monitoring configuration settings, use the **perfmon settings** command in privileged EXEC mode.

perfmon settings

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
	1.1(1)	This command was introduced.

Examples This example shows how to display the **perfmon** settings:

```
hostname# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands	Command	Description
	perfmon	Enables the FWSM to capture performance monitoring information.
	perfmon interval	Sets the performance monitoring capture interval.
	show console-output	Shows the console buffer.
	show perfmon	Displays performance information immediately.

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 FWSM 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:

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

Command History

Release	Modification
3.1(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.

Examples

The following examples show how to configure the **periodic** command:

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 FWSM 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 FWSM 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 FWSM.
default	Restores default settings for the time-range command absolute and periodic keywords.
time-range	Defines access control to the FWSM based on time.

permit (class)

To permit traffic based on the application type, use the **permit** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. The Programmable Intelligent Services Accelerator (PISA) on the switch can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type. To remove the permit statement, use the **no** form of this command.

permit *protocol*

no permit *protocol*

Syntax Description

protocol Specifies a specific protocol, by name or number. For a list of supported protocol names, use the **permit ?** command.

Defaults

By default, all protocols are permitted unless you specifically deny them.

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
4.0(1)	This command was introduced.

Usage Guidelines

Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags using GRE can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to configure multiple upstream switches with PISAs installed.

You might want to deny certain types of application traffic when you want to preserve bandwidth for critical application types. For example, you might deny the use of peer-to-peer (P2P) applications if they are affecting your other critical applications.

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **permit** command (along with **deny** commands) to determine the traffic to permit and deny.

Like access lists, you can combine **permit** and **deny** statements to narrow the traffic that you want denied. By default, all traffic is permitted.

For example, to permit all traffic except for Skype, eDonkey, and Yahoo, enter the following commands:


```
hostname(config-pmap-c) # deny skype
hostname(config-pmap-c) # deny yahoo
hostname(config-pmap-c) # deny eDonkey
```

The following example denies all traffic except for Kazaa and eDonkey:

```
hostname(config-pmap-c) # deny all
hostname(config-pmap-c) # permit kazaa
hostname(config-pmap-c) # permit eDonkey
```

See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for detailed information about PISA integration, including essential information about configuring the switch to work with this feature.

Examples

The following is an example configuration for PISA integration:

```
hostname(config) # access-list BAD_APPS extended permit 10.1.1.0 255.255.255.0 10.2.1.0
255.255.255.0

hostname(config) # class-map denied_apps
hostname(config-cmap) # description "Apps to be blocked"
hostname(config-cmap) # match access-list BAD_APPS

hostname(config-cmap) # policy-map denied_apps_policy
hostname(config-pmap) # class denied_apps
hostname(config-pmap-c) # deny skype
hostname(config-pmap-c) # deny yahoo
hostname(config-pmap-c) # deny eDonkey

hostname(config-pmap-c) # service-policy denied_apps_policy inside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
deny	Denies PISA-tagged traffic.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
show conn	Shows connection information.

permit (gtp-map)

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, or to configure trusted GSNs, use the **permit** command in gtp-map configuration mode. Use the **no** form of this command to remove the command.

permit {**errors** | **response to-object-group** *receive-object-group* **from-object-group** *send-object-group*}

no permit {**errors** | **response to-object-group** *receive-object-group* **from-object-group** *send-object-group*}

Syntax Description	errors	Allows packets with errors to be passed.
	from-object-group <i>send-object-group</i>	Specifies the name of the object group sending the response.
	response	Specifies an object group allowed to receive responses from another object group.
	to-object-group <i>receive-object-group</i>	Specifies the name of the object group sending the requests.

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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.
	3.2(1)	The response keyword was added.

Usage Guidelines	Use the permit command in GTP map configuration mode to allow invalid GTP packets or packets that otherwise would fail parsing and be dropped. You can also configure the trusted GSNs to respond to the requests of a particular GSN not specified in the GTP request. Only object groups with IPv4 address network objects are supported. IPv6 is not supported with GTP.

Examples	The following example permits traffic containing invalid packets or packets that failed, during parsing: <pre>hostname(config)# gtp-map gtp-policy</pre>

```
hostname(config-gtpmap)# permit errors
```

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.

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. This option allows 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.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The PFS setting on the VPN client and the FWSM must match.

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
```

pim

To reenable 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:

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

Command History

Release	Modification
3.1(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)# interface Vlan101
hostname(config-subif)# no pim
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim accept-register

To configure the FWSM 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 <i>acl</i>	Specifies an access list name or number. Use standard host ACLs with this command; extended ACLs are not supported.
route-map <i>map-name</i>	Specifies a route-map name. Use standard host ACLs with the route-maps referenced by 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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM.

pim dr-priority

To configure the neighbor priority on the FWSM 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

<i>number</i>	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 FWSM 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:

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

Command History

Release	Modification
3.1(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)# interface Vlan101
hostname(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
mcast-routing	Enables multicast routing on the FWSM.

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 FWSM 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:

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

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the PIM hello interval to 1 minute:

```
hostname(config)# interface Vlan101
hostname(config-if)# pim hello-interval 60
```

Related Commands	Command	Description
	multicast-routing	Enables multicast routing on the FWSM.

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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the PIM join/prune interval to 2 minutes:

```
hostname(config)# interface Vlan101
hostname(config-if)# pim join-prune-interval 120
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

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 FWSM generates PIM RFC-compliant registers.

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
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM 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 FWSM to use the old checksum calculations:

```
hostname(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

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

<i>acl</i>	(Optional) The name or number of an access list that defines which multicast groups the RP should be used with. This is a standard IP access list.
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.
<i>ip_address</i>	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:

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

Command History

Release	Modification
3.1(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 FWSM 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 FWSM 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:

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

Command History

Release	Modification
3.1(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
mcast-routing	Enables multicast routing on the FWSM.

ping

To determine if other IP addresses are visible from the FWSM, 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 hexadecimal.
<i>host</i>	Specifies the IPv4 or IPv6 address or name of the host to ping.
<i>if_name</i>	(Optional) Specifies the interface name, as configured by the nameif command, by which the <i>host</i> is accessible. If not supplied, then the <i>host</i> 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ping** command allows you to determine if the FWSM has connectivity or if a host is available on the network. If the FWSM has connectivity, ensure that the **icmp permit any interface** command is configured. This configuration is required to allow the FWSM 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 FWSM 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 FWSM 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 FWSM between hosts or routers, but the pings are not successful, use the **capture** command to monitor the success of the ping.

The FWSM **ping** command does not require an interface name. If you do not specify an interface name, the FWSM 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 FWSM:

```
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 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.

policy

To specify the source for retrieving the CRL, use the **policy** command in **crl** configure configuration mode. **Crl** configure configuration mode is accessible from **crypto ca trustpoint** configuration mode. To restore the default setting, use the **no** form of the command.

```

policy {static | cdp | both}

no 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 FWSM 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 FWSM 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 FWSM 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:

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

Command History	Release	Modification
	3.1(1)	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
hostname(ca-crl)#

```


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** 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

<i>name</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(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.
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.

Policy Map Guidelines

See the following guidelines for using policy maps:

- You can only assign one policy map per interface. (However you can create up to 64 policy maps in the configuration.)
- You can apply the same policy map to multiple interfaces.
- You can identify multiple Layer 3/4 class maps in a Layer 3/4 policy map.

- For each class map, you can assign multiple actions from one or more feature types. You can only include multiple **inspect** commands if the class map includes the **match default-inspection-traffic** command.

Supported Feature Types

Feature types supported by the Modular Policy Framework that you can enable in the policy map include the following:

- Connection settings
- Application inspection

Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on whether the service policy is applied to an interface or globally. For a service policy that is applied to an interface, all features are bidirectional; 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. 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.

Feature Matching Guidelines within a Policy Map

See the following guidelines for how a packet matches class maps in a policy 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 FWSM 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 FWSM 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 that includes application inspection, then the second class map actions are not applied.

Feature Matching Guidelines for Multiple Policy Maps

For TCP and UDP traffic (and ICMP when you enable stateful ICMP inspection), service policies operate on traffic flows, and not just individual packets. If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.

For example, if HTTP traffic matches a policy on the inside interface to inspect HTTP traffic, and you have a separate policy on the outside interface for HTTP inspection, then that traffic is not also inspected on the egress of the outside interface. Similarly, the return traffic for that connection will not be inspected by the ingress policy of the outside interface, nor by the egress policy of the inside interface.

For traffic that is not treated as a flow, for example ICMP when you do not enable stateful ICMP inspection, returning traffic can match a different policy map on the returning interface. For example, if you configure connection limits on the inside and outside interfaces, but the inside policy sets the maximum connections to 2000 while the outside policy sets the maximum connections to 3000, then a non-stateful Ping might be denied at a lower level if it is outbound than if it is inbound.

Order in Which Multiple Feature Actions are Applied

Actions within a rule are performed in the following order:

1. Connection settings
2. Application inspection

Default Layer 3/4 Policy Map

The configuration includes a default Layer 3/4 policy map that the FWSM 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 reconfigure 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 FWSM 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

<i>application</i>	Specifies the type of application traffic you want to act upon. Available types include: • dcerpc • esmtplib • http • sip
<i>policy_map_name</i>	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:

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

Command History

Release	Modification
4.0(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.

If a packet matches multiple different **match** or **class** commands, then the order in which the FWSM applies the actions is determined by internal FWSM 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.

```
match request header host length gt 100
  reset
match request method get
  log
```

If an action drops a packet, 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** (or **drop-connection**, and so on.) 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.)

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.

```
match request header length gt 100
  log
match request header length gt 1000
  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. For example, the following three class maps contain two types of **match** commands: **match content length** (higher priority) and **match content type** (lower priority). The sip3 class map includes both commands, but it is ranked according to the lowest priority command, **match content type**. The sip1 class map includes the highest priority command, so it is matched first, regardless of the order in the policy map. The sip3 class map is ranked as being of the same priority as the sip2 class map, which also contains the **match content type** command. They are matched according to the order in the policy map: sip3 and then sip2.

```

class-map inspect type sip match-all sip1
  match content length gt 1000
class-map inspect type sip match-all sip2
  match content type sdp
class-map inspect type sip match-all sip3
  match content length gt 1000
  match content type sdp

policy-map type inspect sip sip
  class sip3
    log
  class sip2
    log
  class sip1
    log

```

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.

polltime interface

To specify the interval between hello packets on the interface, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface *time*

no polltime interface *time*

Syntax Description

time Amount of time between hello messages.

Defaults

The default is 15 seconds.

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
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **polltime interface** command to change the frequency that hello packets are sent out on an interfaces associated with the current failover group. With a faster poll time, the FWSM can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

Five missed consecutive interface hello packets cause interface testing.

This command is available for Active/Active failover only.

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)# polltime interface 20
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Configures the time between hello packets on monitored interfaces.

port-misuse

To restrict HTTP traffic by specifying a restricted application category, use the **port-misuse** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

port-misuse { **im** | **p2p** | **tunneling** | **default** } **action** { **allow** | **reset** | **drop** } [**log**]

no port-misuse { **im** | **p2p** | **tunneling** | **default** } **action** { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	Specifies the action taken when an application in the configured category is detected.
allow	Allows the message.
default	Specifies the default action taken by the FWSM when the traffic contains a supported request method that is not on a configured list.
im	Restricts traffic in the instant messaging application category. The applications checked for are Yahoo Messenger, AIM, and MSN IM.
log	(Optional) Generates a syslog.
p2p	Restricts traffic in the peer-to-peer application category. The Kazaa application is checked.
reset	Sends a TCP reset message to client and server.
tunneling	Restricts traffic in the tunneling application category. The applications checked for are: HTTPPort/HTTHost, GNU Httptunnel, GotoMyPC, Firethru, and Http-tunnel.com Client.

Defaults

This command is disabled by default. When the command is enabled and a supported application category 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		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable the **port-misuse** command, the FWSM applies the specified action to HTTP connections for each supported and configured application category.

The FWSM applies the **default** action to all traffic that does *not* match the application categories 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 application categories with the action of **drop** and **log**, the FWSM drops connections containing the configured application categories, logs each connection, and allows all connections for the other supported application 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 application type with the **allow** action.

Enter the **port-misuse** command once for each setting you wish to apply. You use one instance of the **port-misuse** command to change the default action and one instance to add each application category to the list of configured application types.



Caution

These inspections require searches in the entity body of the HTTP message and may affect the performance of the FWSM.

When you use the **no** form of the 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)# port-misuse p2p drop log
hostname(config-http-map)# exit
```

In this case, only connections in the peer-to-peer category are dropped and the events 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 application 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 im allow
hostname(config-http-map)# exit
```

In this case, only the Instant Messenger application is allowed. When HTTP traffic for the other supported applications is received, the FWSM 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.

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. 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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:

Table 22-1

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	xmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

The following 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.

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

delay 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:

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

Command History

Release	Modification
3.1(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)# 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

<i>/</i>	A required separator between the <i>network</i> and <i>len</i> values.
deny	Denies access for a matching condition.
ge <i>min_value</i>	(Optional) Specifies the minimum prefix length to be matched. The value of the <i>min_value</i> argument must be greater than the value of the <i>len</i> argument and less than or equal to the <i>max_value</i> argument, if present.
le <i>max_value</i>	(Optional) Specifies the maximum prefix length to be matched. The value of the <i>max_value</i> argument must be greater than or equal to the value of the <i>min_value</i> argument, if present, or greater than the value of the <i>len</i> argument if the <i>min_value</i> argument is not present.
<i>len</i>	The length of the network mask. Valid values are from 0 to 32.
<i>network</i>	The network address.
permit	Permits access for a matching condition.
<i>prefix-list-name</i>	The name of the prefix list. The prefix-list name cannot contain spaces.
seq <i>seq_num</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as ip prefix-list).
3.1(1)	This command was changed from ip prefix-list to prefix-list .

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 FWSM begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a match is made, the FWSM 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:

$$len < min\_value \leq max\_value \leq 32$$

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 prefix 10.0.0.0/8:

```
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

<i>prefix-list-name</i>	The name of a prefix list.
<i>text</i>	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
1.1(1)	This command was introduced.

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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all 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-ipsec)# pre-shared-key xyzx
hostname(config-ipsec)#
```

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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:

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

Command History

Release	Modification
3.1(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)# 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.

privilege

To configure the command privilege levels, 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 level for the clear command corresponding to the command specified.
command <i>command</i>	Specifies the command on which to set the privilege level.
configure	(Optional) Sets the privilege level for the command specified.
level <i>level</i>	Specifies the privilege level; valid values are from 0 to 15.
mode enable	(Optional) Indicates that the level is for the enable mode of the command.
mode configure	(Optional) Indicates that the level is for the configure mode of the command.
show	(Optional) Sets the privilege level for the show command corresponding to the command specified.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The privilege command lets you set user-defined privilege levels for the FWSM commands. In particular, this command is useful for setting different privilege levels for related configuration, show, and clear commands. Make sure that you verify privilege level changes in your commands with your security policies before using the new privilege levels.

When commands and users have privilege levels set, the two are compared to determine if a given user can execute a given command. If the user's privilege level is lower than the privilege level of the command, the user is prevented from executing the command.

To change between privilege levels, use the **login** command to access another privilege level and the appropriate **logout**, **exit**, or **quit** command to exit that level.

The **mode enable** and **mode configure** keywords are for commands with both enable and configure modes.

Lower privilege level numbers are lower privilege levels.



Note

The **aaa authentication** and **aaa authorization** commands need to include any new privilege levels that you define before you can use them in your AAA server configuration.

Examples

This example shows how to set the privilege level “5” for an individual user as follows:

```
hostname(config)# username intern1 password pass1 privilege 5
```

This example shows how to define a set of **show** commands with the privilege level “5” as follows:

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
```

This example shows how to apply privilege level 11 to a complete AAA authorization configuration:

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
```

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.
slot	Displays the slot location in the switch.
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:

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

Command History

Release	Modification
3.1(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 module you are logged into when you have multiple modules. During a failover, this feature is useful when both modules have the same hostname.

Examples

The following example shows all available elements in the prompt:

```
hostname(config)# prompt hostname context priority slot state
```

The prompt changes to the following string:

```
hostname/admin/pri/6/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in **crl configure** configuration mode. **Crl configure** configuration mode is accessible from **crypto ca trustpoint** configuration mode. To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

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:

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

Command History

Release	Modification
3.1(1)	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 **crl configure** 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
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
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 **crl configure** configuration mode. **Crl configure** configuration mode is accessible from **crypto ca trustpoint** configuration mode. To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

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 the command:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters **crl configure** 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
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 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** configuration mode. **Crl configure** configuration mode is accessible from **crypto ca trustpoint** configuration mode. To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters **crl configure** 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 esp 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.

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:

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

Command History

Release	Modification
3.1(1)	Support for 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
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

quit through rule Commands

quit

To exit the current configuration mode, or to log out 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM. 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 whose VPN access is authorized by a RADIUS authorization server, 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 *password*

no radius-common-pw

Syntax Description

<i>password</i>	A case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server specified with the aaa-server host command.

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		
	Routed	Transparent	Single	Multiple Context	System
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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 FWSM. Be sure to provide this information to your RADIUS server administrator.

If you do not specify a common user password, each user password is the username of the user. For example, the default RADIUS authorization for a user with the username “jsmith” is “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

The password field is required by the RADIUS protocol and the RADIUS server requires it; however, 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 common 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
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so that 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-with-expiry

To have the FWSM 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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only.

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-ipsec)# radius-with-expiry
hostname(config-ipsec)#
```

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-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

reactivation-mode

To specify the method (reactivation policy) by which failed servers in a group are reactivated, use the **reactivation-mode** command in AAA-server group mode. To remove this specification, use the **no** form of this command:

reactivation-mode depletion [*deadtime minutes*]

reactivation-mode timed

no reactivation-mode

Syntax Description

deadtime <i>minutes</i>	(Optional) Specifies the amount of time that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers.
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. The supported range of values for deadtime is 0-1440 minutes.

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
Aaa-server group	•	•	•	•	—

Command History

Release	Modification
3.1(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. Because UDP is a connectionless protocol,

the FWSM cannot determine if the server is present; therefore, 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 a TACACS+ AAA server named “svrgrp1” to use the depletion reactivation mode, with a deadtime of 15 minutes:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-servers-group)# reactivation-mode depletion deadtime 15
```

The following example configures a TACACS+ AAA server named “svrgrp1” to use timed reactivation mode:

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
```

Related Commands

accounting-mode	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
aaa-server protocol	Enters AAA server group configuration mode so that 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

redistribute

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute {{ **ospf** *pid* **nssa-external** [**1** | **2**]] } | **static** | **connected** } [**metric** *metric_value*]
[**route-map** *map_name*]

no redistribute {{ **ospf** *pid* **nssa-external** [**1** | **2**]] } | **static** | **connected** } [**metric** *metric_value*]
[**route-map** *map_name*]

Syntax Description

connected	Specifies redistributing a network connected to an interface into an EIGRP routing process.
<i>metric metric_value</i>	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
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 .
<i>ospf pid</i>	Used to redistribute an OSPF routing process into the current EIGRP routing process. The <i>pid</i> 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 to apply.
static	Used to redistribute a static route into an EIGRP process.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

This example shows how to redistribute static routes into the current EIGRP process:

```
hostname(config-router)# redistribute static
```

Related Commands

Command	Description
router eigrp	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

redistribute

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **static** | **ospf** *pid* **connected** } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

no redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **static** | **ospf** *pid* **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.
external <i>type</i>	Specifies the metric routes that are external to a specified autonomous system; valid values are 1 or 2 .
internal <i>type</i>	Specifies 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-type <i>metric_type</i>	(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).
metric <i>metric_value</i>	(Optional) Specifies the EIGRP default metric value from 0 to 16777214.
nssa-external <i>type</i>	Specifies the EIGRP metric type for routes that are external to a not-so-stubby area (NSSA); valid values are 1 or 2 .
eigrp <i>pid</i>	Used to redistribute an EIGRP routing process into the current OSPF routing process. The <i>pid</i> specifies the internally used identification parameter for an EIGRP routing process; valid values are from 1 to 65535.
ospf <i>pid</i>	Used to redistribute an OSPF routing process into the current OSPF routing process. The <i>pid</i> specifies the internally used identification parameter for an EIGRP routing process; valid values are from 1 to 65535.
route-map <i>map_name</i>	(Optional) Name of the route map to apply.
static	Used to redistribute a static route into an OSPF process.
subnets	(Optional) For redistributing routes into EIGRP, scopes the redistribution for the specified protocol. If not used, only classful routes are redistributed.
tag <i>tag_value</i>	(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

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

This example shows how to redistribute static routes into the current OSPF process:

```
hostname(config-router)# redistribute static
```

Related Commands

Command	Description
router ospf	Enters router configuration mode. This keyword is only available under router-ospf configuration mode.
show running-config router	Displays the commands in the global router configuration.

redistribute

To configure the type of routes or NAT pools to inject to the MSFC routing tables, use the **redistribute** command in route-inject configuration mode. To delete the configuration, use the **no** form of this command.

redistribute {static | connected | nat} [**route-map** *map-name* | **access-list** *acl-id* | **global-pool** *pool-id*] **interface** *interface-name*

no redistribute

Syntax Description

connected	Injects the connected routes into the MSFC routing table.
nat	Injects a NAT pool into the MSFC routing table.
static	Injects the static routes into the MSFC routing table.
route-map	(Optional) Specifies which routes to inject based on matching a route-map.
<i>map-name</i>	Specifies the name of the route-map to match for the injection.
access-list	(Optional) Specifies which routes to inject based on matching an access list.
<i>acl-id</i>	The unique identifier of the access list to match when you inject the connected and static routes, or NAT pools.
global-pool	(Optional) Specifies the global-pool to inject.
<i>pool-id</i>	The unique identifier of the global-pool.
interface	Specifies the interface on which the routes must be injected.
<i>interface-name</i>	Specifies the name of the interface on which the routes must be injected.

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
Route-inject configuration	•	—	•	• —	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **redistribute** command allows you to configure the type of routes or NAT pools to inject to the MSFC routing tables.

FWSM injects the IP of the FWSM interface as the next-hop IP address for specific destination addresses to the connected and static routes and NAT pools configured on FWSM into the routing table of the local switch.

For example, if you wanted to configure a NAT pool on FWSM, the MSFC and other external routers do not know that those NAT pool addresses are on FWSM unless the user configures the static routes on MSFC to point to the FWSM interface. But by utilizing RHI, you can inject the NAT pool addresses to point to the FWSM interface so the MSFC can automatically forward that traffic to the FWSM.

Because FWSM only supports OSPF or other dynamic routing protocols in single routed-mode, RHI can be used in multi-mode to inject routes (connected/static) to the MSFC, which can then redistribute these routes through OSPF or other dynamic routing protocols. This allows FWSM to redistribute FWSM routes through OSPF or other dynamic routing protocols even when running multi-mode, by utilizing the MSFC's routing protocols and RHI.



Note

The connected and static routes and NAT pools can be selectively injected by configuring a redistribute policy using a standard access list, route-map or global pool ID (only for NAT).

RHI is supported in both single and multi-mode, but not Transparent mode. Additionally, RHI is supported with HA (Active/Standby and Active/Active).

Examples

Configuring RHI for NAT with Standard ACL

In this example, only a perfect match will be injected. The **acl1**, 23.10.143.20/30 is injected with nexthop of 20.22.211.21 (Active IP of “outside”) on vlan 20 (vlan of “outside”).

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.22.211.21 255.255.255.0 standby 20.22.211.22
hostname(config-if)# exit
hostname(config)# access-list acl1 standard permit 23.10.143.20 255.255.255.252
hostname(config)# global (outside) 10 23.10.143.20-23.10.143.23 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.10.143.40-23.10.143.45 netmask 255.255.255.0
hostname(config)# route-inject
hostname(config-route-inject)# redistribute nat access-list acl1 interface outside
```

Configuring RHI for NAT with Global Pool ID

In this example, 23.11.111.1-23.11.111.7 and 23.11.111.10-23.11.111.20 injected with nexthop 20.11.111.11 on vlan 20. Be sure that the global interface and pool ID match the **redistribute** command.

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.11.111.11 255.255.255.0 standby 20.11.111.21
hostname(config-if)# exit
hostname(config)# global (dmz) 10 22.11.111.1-22.11.111.10 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.11.111.1-23.11.111.7 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.11.111.10-23.11.111.20 netmask 255.255.255.0
hostname(config)# global (outside) 20 23.11.111.30-23.11.111.40 netmask 255.255.255.0
hostname(config)# route-inject
hostname(config-route-inject)# redistribute nat global-pool 10 interface outside
```

Configuring RHI for Static Route using route-map

In this example, 23.11.111.0/24 and 25.11.111.0/24 will be injected with nexthop of 20.11.111.11 on vlan 20. The **route-map** command can be used to match destination IP, nexthop IP, metric, or interface

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.11.111.11 255.255.255.0 standby 20.11.111.12
hostname(config-if)# exit
hostname(config)# access-list acl1 standard permit 23.11.111.0 255.255.255.0
hostname(config)# access-list acl2 standard permit 25.11.111.0 255.255.255.0
hostname(config)# route-map map1 permit 10
hostname(config-route-map)# match ip address acl1 acl2
hostname(config-route-map)# exit
hostname(config)# route outside 23.11.111.0 255.255.255.0 23.11.111.9
hostname(config)# route outside 24.11.111.0 255.255.255.0 24.11.111.9
hostname(config)# route outside 25.11.111.0 255.255.255.0 25.11.111.9
hostname(config)# route-inject
hostname(config-route-inject)# redistribute static route-map map1 interface outside
```



Note

Route maps can only be used in single routed mode.

Related Commands

Command	Description
clear configure route-inject	Removes the conditions for the route injection.
route-inject	Allows you to inject the connected and static routes and NAT pools configured on the FWSM into the MSFC routing table.
show route-inject	Displays the routes and NAT pools that have been injected.
show running-config route-inject	Displays the route-injection running configuration.

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

<i>name</i>	Specifies the regular expression name, up to 40 characters in length.
<i>regular_expression</i>	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:

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

Command History

Release	Modification
4.0(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 FWSM 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(ola)g matches dog and dag, but dolag 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 <i>x</i> 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.
<i>char</i>	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.
\xNN	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 FWSM performance when the search length is small.
- The number of regular expression chained tables that need to be searched for a regular expression match.

**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 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.

Command	Description
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 <i>hh:mm</i>	(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.
<i>day</i>	(Optional) Number of the day in the range from 1 to 31.
in [<i>hh:mm</i>]	(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 [<i>hh:mm</i>]	(Optional) Specifies the maximum hold time the FWSM waits to notify other subsystems before a shutdown or reboot. After this time elapses, a quick (forced) shutdown/reboot occurs.
<i>month</i>	(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 FWSM to reload without user confirmation.
quick	(Optional) Forces a quick reload, without notifying or properly shutting down all the subsystems.
reason <i>text</i>	(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
3.1(1)	This command was modified to add the following new arguments and keywords: <i>day</i> , <i>hh</i> , <i>mm</i> , <i>month</i> , quick , save-config , and <i>text</i> .

Usage Guidelines

The **reload** command lets you reboot the FWSM and reload the configuration from Flash.

By default, the **reload** command is interactive. The FWSM first checks whether the configuration has been modified but not saved. If so, the FWSM prompts you to save the configuration. In multiple context mode, the FWSM prompts for each context with an unsaved configuration. If you specify the **save-config** parameter, the configuration is saved without prompting you. The FWSM 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 FWSM 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 FWSM does not check for an unsaved configuration unless you have specified the **save-config** parameter. The FWSM 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 FWSM.

remote-access threshold session-threshold-exceeded

To set threshold values, use the **remote-access threshold session-threshold-exceeded** command in global configuration mode. To remove threshold values, use the **no** version of this command. This command specifies the number of remote access sessions that need to be active for the FWSM to send 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 FWSM 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
3.1(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] [flash:] *source-path* [flash:] *destination-path*

Syntax Description

/noconfirm	(Optional) Suppresses the confirmation prompt.
<i>destination-path</i>	Specifies the path of the destination file.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
<i>source-path</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1(1)	Support for 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

<i>new_name</i>	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:

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

Command History

Release	Modification
3.1(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.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

By default, the FWSM 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 are specific to the server system. Usually used for remote administration.
stou	Disallows the command that stores a file using a unique filename.

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
FTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is used for controlling the commands allowed within FTP requests traversing the FWSM when using strict FTP inspection.

Examples

The following example causes the FWSM 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-method

To restrict HTTP traffic based on the HTTP request method, use the **request-method** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

```
request-method { { ext ext_methods | default } | { rfc rfc_methods | default } } action { allow | reset | drop } [log]
```

```
no request-method { ext ext_methods | rfc rfc_methods } action { allow | reset | drop } [log]
```

Syntax Description

action	Identifies the action taken when a message fails this command inspection.
allow	Allows the message.
default	Specifies the default action taken by the FWSM when the traffic contains a supported request method that is not on a configured list.
drop	Closes the connection.
ext	Specifies extension methods.
<i>ext-methods</i>	Identifies one of the extended methods you want to allow to pass through the FWSM.
log	(Optional) Generates a syslog.
reset	Sends a TCP reset message to client and server.
rfc	Specifies RFC 2616 supported methods.
<i>rfc-methods</i>	Identifies one of the RFC methods you want to allow to pass through the FWSM (see Table 23-2).

Defaults

This command is disabled by default. When the command is enabled and a supported request method 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		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable the **request-method** command, the FWSM applies the specified action to HTTP connections for each supported and configured request method.

The FWSM applies the **default** action to all traffic that does *not* match the request methods on the configured list. The **default** action is to **allow** connections without logging. Given this preconfigured default action, if you specify one or more request methods with the action of **drop** and **log**, the FWSM drops connections containing the configured request methods, logs each connection, and allows all connections containing other supported request methods.

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 method with the **allow** action.

Enter the **request-method** command once for each setting you wish to apply. You use one instance of the **request-method** command to change the default action or to add a single request method to the list of configured methods.

When you use the **no** form of the command to remove a request method from the list of configured methods, any characters in the command line after the request method keyword are ignored.

Table 23-2 lists the methods defined in RFC 2616 that you can add to the list of configured methods:

Table 23-2 RFC 2616 Methods

Method	Description
connect	Used with a proxy that can dynamically switch to being a tunnel (for example SSL tunneling).
delete	Requests that the origin server delete the resource identified by the Request-URI.
get	Retrieves whatever information or object is identified by the Request-URI.
head	Identical to GET except that the server does not return a message-body in the response.
options	Represents a request for information about the communication options available on server identified by the Request-URI.
post	Request that the origin server accept the object enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.
put	Requests that the enclosed object be stored under the supplied Request-URI.
trace	Invokes a remote, application-layer loop-back of the request message.

Examples

The following example provides a permissive policy, using the preconfigured default, which allows all supported request methods that are not specifically prohibited.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc options drop log
hostname(config-http-map)# request-method rfc post drop log
```

In this example, only the **options** and **post** request methods are dropped and the events are logged.

The following example provides a restrictive policy, with the default action changed to **reset** the connection and **log** the event for any request method that is not specifically allowed.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc default action reset log
hostname(config-http-map)# request-method rfc get allow
hostname(config-http-map)# request-method rfc put allow
```

In this case, the **get** and **put** request methods are allowed. When traffic is detected that uses any other methods, the FWSM 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.

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. To return this number to the default of 200, use the **no** form of this command.

request-queue *max_requests*

no request-queue *max_requests*

Syntax Description

<i>max_requests</i>	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:

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

Command History

Release	Modification
3.1(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 gtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

Related Commands

Commands	Description
clear service-policy	Clears global GTP statistics.
inspect gtp	
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.

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:

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

Command History

Release	Modification
4.0(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.

resource acl-partition

To reduce the number of memory partitions in multiple context mode from the maximum of 12, use the **resource acl-partition** command in global configuration mode. To restore the number of partitions to 12, use the **no** form of this command. In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. You might want to reduce the number of partitions to better match the number of contexts you have.

resource acl-partition *number*

no resource acl-partition *number*

Syntax Description

<i>number</i>	Specifies the number of partitions, between 1 and 12.
Note	If you assign a context to a partition, the partition numbering starts with 0. So if you have 12 partitions, the partition numbers are 0 through 11.

Defaults

The FWSM uses 12 memory partitions 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
Global configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.3(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. By default, a context belongs to one of 12 partitions that offers a maximum number rules, including ACEs, AAA rules, and others. See the **resource rule** command for a list of rule limits. The FWSM assigns contexts to the partitions in the order they are loaded at startup. For example, if you have 12 contexts and the maximum number of rules is 14,103, each context is assigned to its own partition, and can use 14,103 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to partition 1, and can use 14,103 rules divided between them; the other 11 contexts continue to use 14,103 rules each. If you delete contexts, the partition membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.



Note

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

You can manually assign a context to a partition with the **allocate-acl-partition** command.

Changing the number of partitions requires you to reload the FWSM. If you are using failover, you must also reload the other failover unit because the memory partitions must match on both units. Traffic loss can occur because both units are down at the same time.

When increasing the number of partitions, the default size of each partition is reduced. If you manually configured the partition sizes using the **size** command, the sizes you set might not be compatible with the new smaller partition sizes. If the current configured sizes do not fit into the new partitions, then the FWSM rejects the **resource acl-partition** command. The FWSM also checks the rule allocation (see the **resource rule** or **rule** command). If you manually allocated rules between features so that the total number of rules allocated is now greater than those available, then the FWSM rejects the **resource acl-partition** command. Similarly, if the absolute maximum number of rules for a feature is now exceeded, then the FWSM rejects the **resource acl-partition** command.

Examples

The following example partitions the memory into 8 parts:

```
hostname(config)# resource acl-partition 8
```

```
WARNING: This command leads to re-partitioning of ACL Memory.  
It will not take affect until you save the configuration and reboot.
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.

resource partition

To customize a memory partition, including changing the size or reallocating rules between features, use the **resource partition** command in global configuration mode. To remove the resource partition configuration, use the **no** form of this command.

resource partition *number*

no resource partition *number*

Syntax Description

number Specifies the partition number, between 0 and 11 by default. If you changed the number of partitions using the **resource acl-partition** command, the partition numbering starts with 0. So if you have 10 partitions, the partition numbers are 0 through 9.

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
4.0(1)	This command was introduced.

Usage Guidelines

After you enter resource partition configuration mode, you can customize the partition using the **size** and **rule** commands, for example.

Examples

The following example enters resource partition configuration mode, and changes the size 5000 rules:

```
hostname(config)# resource partition 0
hostname(config-partition)# size 5000
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.

Command	Description
resource acl-partition	Sets the total number of memory partitions.
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource partition	Shows the memory partition sizes.
show resource rule	Shows the current allocation of rules.
show running-config resource partition	Shows the current memory partition configuration.
size	Changes the size of a memory partition.

resource rule

To reallocate rules between features, use the **resource rule** command in global configuration mode. To restore the default values, use the **no** form of this command. There are a fixed number of rules available on the FWSM, so you might want to reallocate rules between features depending on usage. Features that use rules include access lists, inspections, AAA, and more.

```
resource rule nat {max_policy_nat_rules | current | default | max}
    acl {max_ace_rules | current | default | max}
    filter {max_filter_rules | current | default | max}
    fixup {max_inspect_rules | current | default | max}
    est {max_established_rules | current | default | max}
    aaa {max_aaa_rules | current | default | max}
    console {max_console_rules | current | default | max}
```

no resource rule

Syntax Description

aaa <i>max_aaa_rules</i>	Sets the maximum number of AAA rules, between 0 and 10000.
acl <i>max_ace_rules</i>	Sets the maximum number of ACEs, between 0 and 74188.
console <i>max_console_rules</i>	Sets the maximum number of ICMP, Telnet, SSH, and HTTP rules, between 0 and 4000.
current	Keeps the current value set.
default	Sets the maximum rules to the default. To view the defaults, use the show resource rule command.
est <i>max_established_rules</i>	Sets the maximum number of established commands, between 0 and 716. The established command creates two types of rules, control and data. You allocate both rules by setting the number of established commands; you do not set each rule separately. However, both of these types are shown in the show resource rule and show np 3 acl count displays, so be sure to double the est value when comparing the total number of rules configured with the display in the show commands.
filter <i>max_filter_rules</i>	Sets the maximum number of filter rules, between 0 and 6000.
fixup <i>max_inspect_rules</i>	Sets the maximum number of inspect rules, between 0 and 10000.
max	Sets the rules to the maximum allowed for the feature. Be sure to set other features lower to accommodate this value.
nat <i>max_policy_nat_rules</i>	Sets the maximum number of policy NAT ACEs, between 0 and 10000.

Defaults

Use the **show resource rule** command to view default 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
3.2(1)	This command was introduced.

Usage Guidelines

If you increase the value for one feature, then you must decrease the value by the same amount for one or more features so the total number of rules does not exceed the system limit. Use the **show resource rule** command to view the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature.

You must enter all arguments in this command.

This command takes effect immediately.

If you increase the size of a partition (the **size** command, or if you decrease the number of partitions using the **resource acl-partition** command) but have not yet reloaded, the maximum number of rules remains at the old smaller size. You have to reload to see the increased limits. If you decrease the size of a partition but have not yet reloaded, the new smaller number of rules is reflected right away.

To view the number of rules currently being used so you can plan your reallocation, enter one of the following commands.

- In single mode or within a context, enter the following command:

```
hostname(config)# show np 3 acl count
```

- In multiple context mode system execution space, enter the following command:

```
hostname(config)# show np 3 acl count partition_number
```

For example, the following display shows the number of inspections (Fixup Rule) close to the maximum of 9216. You might choose to reallocate some access list rules (ACL Rule) to inspections.

```
hostname(config)# show np 3 acl count
```

```
----- CLS Rule Current Counts -----
CLS Filter Rule Count      :          0
CLS Fixup Rule Count       :        9001
CLS Est Ctl Rule Count     :           4
CLS AAA Rule Count         :          15
CLS Est Data Rule Count    :           4
CLS Console Rule Count     :          16
CLS Policy NAT Rule Count  :           0
CLS ACL Rule Count         :       30500
CLS ACL Uncommitted Add    :           0
CLS ACL Uncommitted Del    :           0
...
```

Rules in Multiple Context Mode

In multiple context mode with the default of 12 memory partitions, each context supports the maximum number of rules; the actual number of rules supported in a context might be more or less, depending on how many contexts you have and how many partitions you configure. See the **resource acl-partition** command for information about memory distribution among contexts.

If you reduce the number of partitions, the maximum number of rules is recalculated and might not match the total system number available for 12 partitions. To view the maximum number of rules for partitions, enter the following command in the system execution space:

```
hostname(config)# show resource rule
```

For example, the following display shows the maximum rules as 19219 per partition with 12 partitions (this is an example only, and might differ from the actual number of rules for your system):

```
hostname(config)# show resource rule
```

CLS Rule	Default Limit	Configured Limit	Absolute Max
Policy NAT	384	384	833
ACL	14801	14801	14801
Filter	576	576	1152
Fixup	1537	1537	3074
Est Ctl	96	96	96
Est Data	96	96	96
AAA	1345	1345	2690
Console	384	384	768
Total	19219	19219	

```
Partition Limit - Configured Limit = Available to allocate
19219 - 19219 = 0
```

To override the global setting for rule reallocation, use the rule command to set the **rule** allocation for a specific partition.

Examples

The following example reallocates 1000 rules from the single-mode default 74,188 ACEs to inspections (default 4147):

```
hostname(config)# resource rule nat default acl 73188 filter default fixup 5157 est
default aaa default console default
```

In multiple context mode with 12 partitions, to reallocate 100 ACEs (default 10,633) to inspections (default 1417) as well as all but one established rule (default 70) to filter (default 425), enter the following command:

```
hostname(config)# resource rule nat default acl 10533 filter 494 fixup 1517 est 1 aaa
default console default
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.

Command	Description
resource acl-partition	Sets the number of memory partitions for rules.
rule	Sets the resource rule allocation for a specific partition.
show np 3 acl count	Shows the number of rules in use.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.
show resource rule	Shows the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature.

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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the FWSM waits between connection attempts. Use the **timeout** command to specify the length of time during which the FWSM 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
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so that 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 FWSM attempts to make a connection to a AAA server.

re-xauth

To require that 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 | disable}

no re-xauth

Syntax Description

disable	Disables reauthentication on IKE rekey
enable	Enables reauthentication on IKE rekey

Defaults

Reauthentication on IKE rekey is disabled.

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
Group policy	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If you enable reauthentication on IKE rekey, the FWSM 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.

If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. In this case, disable reauthentication. 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

To enable and change RIP settings, use the **rip** command in global configuration mode. To disable the FWSM RIP routing table updates, use the **no** form of this command.

rip *if_name* { **default** | **passive** } [**version** { **1** | **2** [**authentication** { **text** | **md5** } *key* *key_id*]]

no rip *if_name* { **default** | **passive** } [**version** { **1** | **2** [**authentication** { **text** | **md5** } *key* *key_id*]]

Syntax Description

authentication	(Optional) Enables RIP version 2 authentication.
default	Broadcast a default route on the interface.
<i>if_name</i>	The interface on which RIP is being enabled.
<i>key</i>	Key to authenticate RIP updates.
<i>key_id</i>	Key identification value; valid values range from 1 to 255.
md5	Uses MD5 for RIP message authentication.
passive	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.
text	Uses clear text for RIP message authentication (not recommended).
version	(Optional) Specifies the RIP version; valid values are 1 and 2 .

Defaults

RIP is disabled.

If you do not specify a version, RIP version 1 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **rip** command lets you to enable the sending and receiving of RIP routing updates on an interface. You configure RIP update transmission and reception independently; you can enable transmission only, reception only, or both transmission and reception on each interface. Use the **passive** keyword with the **rip** command to enable RIP update reception. Use the **default** keyword with the **rip** command to enable the broadcast of a default route. To enable both transmission and reception of RIP updates on an

interface, you must two **rip** commands for the interface, one with the **default** keyword, enabling the sending of RIP routing updates, and one with the **passive** keyword, enabling the interface to receive RIP updates and to populate the routing table with those updates.

**Note**

The FWSM cannot pass RIP updates between interfaces.

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.

Configuring RIP Version 2 registers the multicast address 224.0.0.9 on the respective interface to be able to accept multicast RIP Version 2 updates. When RIP Version 2 is configured in passive mode, the FWSM accepts RIP Version 2 multicast updates with an IP destination of 224.0.0.9. When RIP Version 2 is configured in default mode, the FWSM transmits default route updates using an IP multicast destination of 224.0.0.9. Removing the RIP version 2 commands for an interface unregisters the multicast address from the interface card.

**Note**

Only Intel 10/100 and Gigabit interfaces support multicasting.

RIP is not supported under transparent mode. By default, the FWSM denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through a FWSM 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 like `access-list myriplist extended permit ip any host 224.0.0.9`. To permit RIP version 1 broadcasts, create an access list entry like `access-list myriplist extended permit udp any any eq rip`. Apply these access list entries to the appropriate interface using the **access-group** command.

Examples

The following example shows how to combine version 1 and version 2 commands and list the information with the **show running-config rip** command after entering the **rip** commands. The **rip** commands let you to do the following.

- Enable version 2 passive and default RIP using MD5 authentication on the outside interface to encrypt the key that is used by the FWSM and other RIP peers, such as routers.
- Enable version 1 passive RIP listening on the inside interface of the FWSM.
- Enable version 2 passive RIP listening on the dmz (demilitarized) interface of the FWSM.

```
hostname(config)# rip outside passive version 2 authentication md5 thisisakey 2
hostname(config)# rip outside default version 2 authentication md5 thisisakey 2
hostname(config)# rip inside passive
hostname(config)# rip dmz passive version 2
```

```
hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

The following example shows how to use the version 2 feature that passes the encryption key in text form:

```
hostname(config)# rip out default version 2 authentication text thisisakey 3
hostname# show running-config rip
```

```
rip outside default version 2 authentication text thisisakey 3
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.
debug rip	Displays debug information for RIP.
show running-config rip	Displays the RIP commands in the running configuration.

rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

rmdir [/noconfirm] [flash:]*path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
flash:	(Optional) Specifies the nonremovable internal Flash, followed by a colon.
<i>path</i>	(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:

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

Command History

Release	Modification
3.1(1)	Support for 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]*

no route *interface_name ip_address netmask gateway_ip [metric]*

Syntax Description

<i>gateway_ip</i>	Specifies the IP address of the gateway router (the next-hop address for this route).
	Note The <i>gateway_ip</i> argument is optional in transparent mode.
<i>interface_name</i>	Internal or external network interface name.
<i>ip_address</i>	Internal or external network IP address.
<i>metric</i>	(Optional) The administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
<i>netmask</i>	Specifies a network mask to apply to <i>ip_address</i> .

Defaults

The *metric* default is 1.

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
1.1(1)	This command was introduced.

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.

Create static routes to access networks that are connected outside a router on any interface. For example, the FWSM 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 FWSM 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 FWSM as the gateway IP address, the FWSM 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
```

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-inject

To inject the connected and static routes and NAT pools configured on FWSM into the MSFC routing table, use the **route-inject** command in global configuration mode. To delete the connection, use the **no** form of this command or the **clear configure route-inject** command.

route-inject

no route-inject

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
Global configuration	•	—	•	• —	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **route-inject** command allows you to inject the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.

FWSM injects the IP address of the FWSM interface as the next-hop IP address for specific destination addresses to the connected and static routes and NAT pools configured on FWSM into the routing table of the local switch.

For example, if you wanted to configure a NAT pool on FWSM, the MSFC and other external routers do not know that those NAT pool addresses are on FWSM unless the user configures the static routes on MSFC to point to the FWSM interface. But by utilizing RHI, you can inject the NAT pool addresses to point to the FWSM interface so the MSFC can automatically forward that traffic to the FWSM.

Because FWSM only supports OSPF or other dynamic routing protocols in single routed-mode, RHI can be used in multi-mode to inject routes (connected/static) to the MSFC, which can then redistribute these routes through OSPF or other dynamic routing protocols. This allows FWSM to redistribute FWSM routes through OSPF or other dynamic routing protocols even when running multi-mode, by utilizing the MSFC routing protocols and RHI.

**Note**

The connected and static routes and NAT pools can be selectively injected by configuring a redistribute policy using a standard access-list, route-map or global pool ID (only for NAT).

RHI is supported in both single and multi-mode, but not Transparent mode. Additionally, RHI is supported with HA (Active/Standby and Active/Active).

Examples

Configuring RHI for NAT with Standard ACL

- Step 5** In this example, only a perfect match will be injected. The **acl1**, 23.10.143.20/30 is injected with nexthop of 20.22.211.21 (Active IP of “outside”) on vlan 20 (vlan of “outside”).

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.22.211.21 255.255.255.0 standby 20.22.211.22
hostname(config-if)# exit
hostname(config)# access-list acl1 standard permit 23.10.143.20 255.255.255.252
hostname(config)# global (outside) 10 23.10.143.20-23.10.143.23 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.10.143.40-23.10.143.45 netmask 255.255.255.0
hostname(config)# route-inject
hostname(config-route-inject)# redistribute nat access-list acl1 interface outside
```

Configuring RHI for NAT with Global Pool ID

- Step 6** In this example, 23.11.111.1-23.11.111.7 and 23.11.111.10-23.11.111.20 injected with nexthop 20.11.111.11 on vlan 20. Be sure that the global interface and pool ID match the **redistribute** command.

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.11.111.11 255.255.255.0 standby 20.11.111.21
hostname(config-if)# exit
hostname(config)# global (dmz) 10 22.11.111.1-22.11.111.10 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.11.111.1-23.11.111.7 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.11.111.10-23.11.111.20 netmask 255.255.255.0
hostname(config)# global (outside) 20 23.11.111.30-23.11.111.40 netmask 255.255.255.0
hostname(config)# route-inject
hostname(config-route-inject)# redistribute nat global-pool 10 interface outside
```

Configuring RHI for Static Route using route-map

In this example, 23.11.111.0/24 and 25.11.111.0/24 will be injected with nexthop of 20.11.111.11 on vlan 20. The **route-map** command can be used to match destination IP, nexthop IP, metric, or interface.

```
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.11.111.11 255.255.255.0 standby 20.11.111.12
hostname(config-if)# exit
hostname(config)# access-list acl1 standard permit 23.11.111.0 255.255.255.0
hostname(config)# access-list acl2 standard permit 25.11.111.0 255.255.255.0
hostname(config)# route-map map1 permit 10
hostname(config-route-map)# match ip address acl1 acl2
hostname(config-route-map)# exit
hostname(config)# route outside 23.11.111.0 255.255.255.0 23.11.111.9
```

```
hostname(config)# route outside 24.11.111.0 255.255.255.0 24.11.111.9
hostname(config)# route outside 25.11.111.0 255.255.255.0 25.11.111.9
hostname(config)# route-inject
hostname(config-route-inject)# redistribute static route-map map1 interface outside
```

**Note**

Route maps can only be used in single routed mode.

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
debug route-inject	Enables debugging of the route-injections that have been configured on the FWSM.
redistribute	Configures the type of route or NAT pools to inject.
show route-inject	Displays the routes and NAT pools that have been injected.
show running-config route-inject	Displays the route-injection running configuration.

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.
<i>map_tag</i>	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.
<i>seq_num</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

route-monitor

To monitor routes and switch to an alternate path in the event a router goes down, use the **route-monitor** command in interface configuration mode. To remove route monitoring, use the **no** form of this command.

route-monitor *network_address network_mask* [**query interval** *interval*] [**max-failures** *failures*]

no route-monitor *network_address network_mask* [**query interval** *interval*] [**max-failures** *failures*]

Syntax Description

max-failures <i>failures</i>	(Optional) Specifies the number of ICMP queries that are not replied to before the route is considered down. Valid values are between 3 and 200; the default value is 5.
<i>network address</i>	Specifies the network address to be monitored.
<i>network mask</i>	Specifies the network mask for the address to be monitored.
query interval <i>interval</i>	(Optional) Specifies the interval value in milliseconds. Valid values are between 100 or 3000 ; the default value is 300.

Defaults

The default value for maximum number of failures is 5, and the default value for query intervals is 300 milliseconds.

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
Interface configuration	•	•	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines



Note

Currently, you can only monitor routes for one network as specified in the **route-monitor** command.

If you configured multiple static or default routes, FWSM lets you configure multiple routes to monitor whether there are any problems on the active route, and if so, switches to an alternate route on the network in the event a router goes down.

To do this, FWSM route monitoring process starts to send out ICMP queries to determine the best two static route for the destination network and a back up route at a configurable interval of time set. The interval of sending the ICMP query is set by the *interval* keyword; valid values are 100 to 3000, with the default value at 300 milliseconds. The query is always sent to both of the chosen routers, keeping the current available status locally.

The two routes chosen have the least metric distance, with the lowest chosen as the best path to send traffic. In the FWSM, the **route-monitor** command will automatically choose the best two routes among the static routes configured. The next best path always gets installed in the routing table when the current route goes down, and the current one becomes the backup router.

If the ICMP query does not receive a configurable threshold number set by the *failures* keyword, the router is determined to be unreachable. The *failures* keyword is the maximum number of ICMP queries that are not replied to before the router is determined to be down; the default value being five seconds. At this point the backup route takes precedence, provided this route was reachable, and becomes the best route. The original route then becomes the backup route.

If the original best route becomes reachable again, then FWSM switches back to that route and the current best route becomes the backup route. If in case both routes become unreachable, then both are made backup routes. However, there is no change in the routing table.

To monitor a static or default route, enter the following command:

```
hostname(config-if)# route-monitor network_address network_mask [query_interval interval]
[max-failures failures]
```

Examples

This example shows how to monitor a static route:

```
hostname(config-if)# route-monitor 255.255.255.0
```

Related Commands

Command	Description
show running-config router	Displays the commands in the global router configuration.

router bgp

To start a BGP routing process and configure parameters for that process, use the **router bgp** command in global configuration mode. To disable BGP routing, use the **no** form of this command.

router bgp *as-number*

no router bgp *as-number*

Syntax Description

<i>as-number</i>	Number of an autonomous system that identifies the FWSM to other BGP routers and tags the routing information passed along. The <i>as-number</i> assigned to the BGP stub routing process must be the same as the BGP neighbor <i>as-number</i> .

Defaults

BGP routing is disabled.

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 ¹	System
Global configuration	•	—	•	•	—

1. This command is only available in the admin context.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

The **router bgp** command is the global configuration command for BGP routing processes running on the FWSM. Once you enter the **router bgp** command, the command prompt appears as `hostname(config-router)#`, indicating that you are in router configuration mode. The **no router bgp** command terminates the BGP routing process.

The AS number assigned to the BGP stub routing process must be the same as the BGP neighbor AS number.

The **router bgp** command is used with the following BGP-specific commands to configure BGP routing process:

- **bgp router id**—Specified the BGP router ID for the FWSM.
- **neighbor**—Specifies the neighbor BGP router.
- **network**—Specifies the networks that can be advertised by the BGP routing process.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples

The following example shows how to enter the configuration mode for the BGP routing process. The FWSM belongs to AS 800:

```
hostname(config)# router bgp 800  
hostname(config-router)#
```

Related Commands

Command	Description
bgp router-id	Specifies the BGP router ID for the FWSM.
clear configure router	Clears the router commands from the running configuration.
neighbor remote-as	Specifies the neighbor BGP router.
network	Specifies the networks that can be advertised by the BGP routing process.
show running-config router	Displays the router commands in the running configuration.

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

<i>as-number</i>	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:

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

Command History

Release	Modification
4.0(1)	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 FWSM.

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 FWSM 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 FWSM.
- **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 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.

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

<i>pid</i>	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The <i>pid</i> 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the FWSM. 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 FWSM. 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.

You cannot configure OSPF when RIP is configured on the FWSM.

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-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 FWSM is used as the router ID.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the highest-level IP address on the FWSM is a private address, then this address is sent in hello packets and database definitions. To prevent this address from being used, 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.

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.

rule

To reallocate rules between features for a specific memory partition in multiple context mode, use the **rule** command in resource partition configuration mode. To restore the default values, use the **no** form of this command. There are a fixed number of rules available on the FWSM, so you might want to reallocate rules between features depending on usage. Features that use rules include access lists, inspections, AAA, and more.

```
rule nat {max_policy_nat_rules | current | default | max}
    acl {max_ace_rules | current | default | max}
    filter {max_filter_rules | current | default | max}
    fixup {max_inspect_rules | current | default | max}
    est {max_established_rules | current | default | max}
    aaa {max_aaa_rules | current | default | max}
    console {max_console_rules | current | default | max}
```

no rule

Syntax Description

aaa <i>max_aaa_rules</i>	Sets the maximum number of AAA rules, between 0 and 10000.
acl <i>max_ace_rules</i>	Sets the maximum number of ACEs, between 0 and 74188.
console <i>max_console_rules</i>	Sets the maximum number of ICMP, Telnet, SSH, and HTTP rules, between 0 and 4000.
current	Keeps the current value set.
default	Sets the maximum rules to the default. To view the defaults, use the show resource rule command.
est <i>max_established_rules</i>	Sets the maximum number of established commands, between 0 and 716. The established command creates two types of rules, control and data. You allocate both rules by setting the number of established commands; you do not set each rule separately. However, both of these types are shown in the show resource rule and show np 3 acl count displays, so be sure to double the est value when comparing the total number of rules configured with the display in the show commands.
filter <i>max_filter_rules</i>	Sets the maximum number of filter rules, between 0 and 6000.
fixup <i>max_inspect_rules</i>	Sets the maximum number of inspect rules, between 0 and 10000.
max	Sets the rules to the maximum allowed for the feature. Be sure to set other features lower to accommodate this value.
nat <i>max_policy_nat_rules</i>	Sets the maximum number of policy NAT ACEs, between 0 and 10000.

Defaults

Use the **show resource rule** command to view default 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
Resource partition configuration	•	•	—	—	•

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If you increase the value for one feature, then you must decrease the value by the same amount for one or more features so the total number of rules does not exceed the system limit. Use the **show resource rule partition** command to view the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature.

You must enter all arguments in this command.

This command takes effect immediately.

This command overrides the global allocation settings set by the **resource rule** command.

If you increase the size of a partition (the **size** command, or if you decrease the number of partitions using the **resource acl-partition** command) but have not yet reloaded, the maximum number of rules remains at the old smaller size. You have to reload to see the increased limits. If you decrease the size of a partition but have not yet reloaded, the new smaller number of rules is reflected right away.

To view the total number of rules available per partition, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature, enter the following command:

```
hostname(config)# show resource rule partition number
```

For example, the following display shows the maximum rules as 19219 for partition 0 (this is an example only, and might differ from the actual number of rules for your system):

```
hostname(config)# show resource rule partition 0
```

CLS Rule	Default Limit	Configured Limit	Absolute Max
Policy NAT	384	384	833
ACL	14801	14801	14801
Filter	576	576	1152
Fixup	1537	1537	3074
Est Ctl	96	96	96
Est Data	96	96	96
AAA	1345	1345	2690
Console	384	384	768
Total	19219	19219	

Partition Limit - Configured Limit = Available to allocate
 19219 - 19219 = 0

To view the number of rules currently being used so you can plan your reallocation, enter the following command:

```
hostname(config)# show np 3 acl count partition_number
```

For example, the following display shows the number of inspections (Fixup Rule) close to the maximum of 9216. You might choose to reallocate some access list rules (ACL Rule) to inspections.

```
hostname(config)# show np 3 acl count

----- CLS Rule Current Counts -----
CLS Filter Rule Count      :          0
CLS Fixup Rule Count       :        9001
CLS Est Ctl Rule Count     :           4
CLS AAA Rule Count        :          15
CLS Est Data Rule Count    :           4
CLS Console Rule Count     :          16
CLS Policy NAT Rule Count  :           0
CLS ACL Rule Count        :       30500
CLS ACL Uncommitted Add   :           0
CLS ACL Uncommitted Del   :           0
...
```

Examples

The following example for partition 0 reallocates 999 rules from the default 14,801 ACEs to inspections (default 9001):

```
hostname(config)# resource partition 0
hostname(config-partition)# rule nat default acl 13802 filter default fixup 10000 est
default aaa default console default
```

Examples

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
resource acl-partition	Sets the number of memory partitions for rules.
resource rule	Sets the resource rule allocation globally.
show np 3 acl count	Shows the number of rules in use.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.
show resource rule	Shows the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature.



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

By default, these behaviors are disabled.

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
2.2(1)	This command with the inter-interface keyword was introduced.
2.3(1)	Support for the intra-interface keyword was added.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) lets you 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).

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed.



Note

If you use a same-security interface for both the outside and inside interfaces, you might want to enable the **xlate-bypass** command; in some situations, you can exceed the maximum number of xlates using that configuration (see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for limits). For example, without **xlate-bypass**, the FWSM creates xlates for all connections (even if you do not configure NAT). In a same-security-traffic configuration, the FWSM randomly chooses which same-security interface is the “inside” interface for the sake of creating xlates. If the FWSM considers the outside same-security interface as the “inside” interface, it creates

xlates for every Internet host being accessed through it. If there is any application (or a virus) on the internal network that scans thousands of Internet hosts, all entries in the xlate table may be quickly exhausted.

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.

sdi-pre-5-slave

To specify the IP address or name of an optional SDI AAA “slave” server to use for this host connection that uses a version of SDI prior to SDI version 5, use the **sdi-pre-5-slave** command in AAA-server host configuration mode. To remove this specification, use the **no** form of this command:

sdi-pre-5-slave *host*

no sdi-pre-5-slave

Syntax Description

host Specify the name or IP address of the slave server host.

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
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is available for any host in an SDI AAA server group, but it is relevant only if the SDI version for the host is set to sdi-pre-5 in the **sdi-version** command. Prior to using this command, you must have configured the AAA server to use the SDI protocol.

The **sdi-pre-5-slave** command lets you identify an optional secondary server that is to be used if the primary server fails. The address specified by this command must be that of a server that is configured as a “slave” to the primary SDI server. In this situation, if you are using a pre-5 version, you must configure the **sdi-pre-5-slave** command so that the FWSM can access the appropriate SDI configuration record that is downloaded from the server. This is not an issue with version 5 and later versions.

Examples

The following example configures the AAA SDI server group “svrgrp1” that uses an SDI version prior to SDI version 5.

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# sdi-version sdi-pre-5
hostname(config-aaa-server-host)# sdi-pre-5-slave 209.165.201.31
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA server configurations.
sdi-version	Specifies the version of SDI to use for this host connection.
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

sdi-version

To specify the version of SDI to use for this host connection, use the **sdi-version** command in AAA-server host configuration mode. To remove this specification, use the **no** form of this command:

sdi-version *version*

no sdi-version

Syntax Description

<i>version</i>	Specify the version of SDI to use. Valid values are: sdi-5—SDI version 5.0 (default) sdi-pre-5—SDI versions prior to 5.0

Defaults

The default version is **sdi-5**.

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
Aaa-server host	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is valid only for SDI AAA servers. If you configure a secondary (failover) SDI AAA server, and if the SDI version for that server is earlier than version 5, you must also specify the **sdi-pre-5-slave** command.

Examples

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
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 host	Enter AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.

clear configure aaa-server	Remove all AAA 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

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:

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

Command History

Release	Modification
3.1(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 that 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)# 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.

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 {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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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 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 FWSM, 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 FWSM 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

<i>number</i>	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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced. It moved from a keyword of the nameif command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- 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 FWSM.
- 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
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 gigabitethernet1
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.

serial-number

To include the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the FWSM serial number in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example configures an SDI AAA server named “svrgrp1” to use server port number 8888:

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 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

service reset no-connection

To send a reset for a TCP packet for which the FWSM does not have any connection history, use the **service reset no-connection** command in global configuration mode. To disable sending a reset, use the **no** form of this command.

service reset no-connection

no service reset no-connection

Syntax Description

This command has no arguments or keywords.

Defaults

By default, resets are sent.

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
4.0(1)	This command was introduced.

Usage Guidelines

If the FWSM receives an ACK or SYN-ACK packet without first receiving a SYN packet, then the FWSM does not have any connection history for the packet. By default, the FWSM sends a RST for the packet. To disable the sending of the RST, enter the **no service reset no-connection** command.

See the **service reset inbound** command to set the reset behavior for SYN packets that attempt to establish a connection with the FWSM but are denied based on access lists or AAA configuration.

Examples

The following example shows how to disable the sending of the RST:

```
hostname(config)# no service reset no-connection
```

Related Commands

Command	Description
service reset inbound	Sets whether to send a reset for TCP SYN packets that are denied.
show running-config service	Displays the system services.

service resetinbound

To send a reset to inbound TCP connections when they are denied, use the **service resetinbound** command in global configuration mode. To not send a reset, use the **no** form of this command.

service resetinbound

no service resetinbound

Syntax Description

This command has no arguments or keywords.

Defaults

By default, no resets are sent.

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
1.1(1)	This command was introduced.

Usage Guidelines

The **service resetinbound** command works with all inbound TCP connections whose access lists or uauth (user authorization) do not allow inbound connections. One use is for resetting identity request (IDENT) connections. If an inbound TCP connection is attempted and denied, you can use the **service resetinbound** command to return an RST (reset flag in the TCP header) to the source. Without the keyword, the FWSM drops the packet without returning an RST.

To configure whether to send a reset for packets that do not have a connection on the FWSM, see the **service reset no-connection** command. For example, if the FWSM receives an ACK or SYN-ACK packet without first receiving a SYN packet, then the FWSM does not have any connection history for the packet. The **service resetinbound** command applies only to SYN packets that attempt to establish a connection with the FWSM.

The FWSM sends a TCP RST to the host connecting inbound and stops the incoming IDENT process so that outbound e-mail can be transmitted without having to wait for IDENT to time out. The FWSM sends a syslog message stating that the incoming connection was denied. Without entering the **service resetinbound** command, the FWSM drops packets that are denied and generates a syslog message stating that the SYN was denied. However, outside hosts keep retransmitting the SYN until the IDENT times out.

When an IDENT connection times out, the connections slow down. Perform a trace to determine that IDENT is causing the delay and then enter the **service** command.

Use the **service resetinbound** command to handle an IDENT connection through the FWSM. These methods for handling IDENT connections are ranked from most secure to the least secure:

1. Use the **service resetinbound** command.
2. Use the **established** command with the **permitto tcp 113** keyword.
3. Enter the **static** and **access-list** commands to open TCP port 113.

When using the **aaa** command, 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 is as follows:

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

The following is the expected behavior of traffic on the FWSM in regards to the reset flag.

1. If **resetinbound** is configured and if denied traffic flows from a low security interface to high security interface, then a reset is sent.
2. If **resetinbound** is configured and if denied traffic flows from an interface to another interface with the same security, then a reset is sent.
3. If **resetinbound** is not configured and if denied traffic flows from high security interface to low security interface, then a reset is sent.

Examples

This example shows how to enable system services:

```
hostname(config)# service resetinbound
```

Related Commands

Command	Description
show running-config service	Displays the system services.

service-policy

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 *polymap_name* [**global** | **interface** *intf*]

no service-policy *polymap_name* [**global** | **interface** *intf*]

Syntax Description

<i>polymap_name</i>	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 <i>intf</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Interface service policies take precedence over the global service policy.

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 FWSM interfaces:

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

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.
clear service-policy	Clears service policy statistics.
clear configure service-policy	Clears service policy configurations.

set boot device (Catalyst OS)

By default, the FWSM boots from the **cf:4** application partition. However, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. To change the default boot partition, enter the **set boot device** command in privileged EXEC mode.

set boot device cf:n mod_num

Syntax Description	
<i>mod_num</i>	Specifies the module number. Use the show module command to view installed modules and their numbers.
cf:n	Sets the boot partition. Application partitions include cf:4 and cf:5 . The maintenance partition is cf:1 .

Defaults	The default boot partition is cf:4.

Command Modes	Privileged EXEC.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines	Each application partition has its own startup configuration.

To view the current boot partition, enter the **show boot device** command:

```

Console> show module
Mod Slot Ports Module-Type           Model              Sub Status
---
1    1    2    1000BaseX Supervisor      WS-X6K-SUP1A-2GE   yes  ok
15   1    1    Multilayer Switch Feature WS-F6K-MSFC        no   ok
4    4    2    Intrusion Detection Syste WS-X6381-IDS       no   ok
5    5    6    Firewall Module          WS-SVC-FWM-1       no   ok
6    6    8    1000BaseX Ethernet       WS-X6408-GBIC      no   ok

```

Examples	The following example shows how to set the boot partition to the maintenance partition:

```
Console> (enable) set boot device cf:1 1
```

Related Commands	Command	Description
	reset	Resets the module.
	show boot device	Shows the boot partitions of each module.
	show module	Shows all installed modules.

set connection

To set the maximum TCP and UDP connections, connection rate limits, or disable TCP sequence number randomization for a traffic class, use the **set connection** command in class configuration mode. The class configuration mode is accessible from the policy-map configuration mode. To remove these specifications, use the **no** form of this command.

```
set connection {[conn-max number] [conn-rate-limit number] [random-seq# {enable | disable}]}
```

```
no set connection {[conn-max number] [conn-rate-limit number] [random-seq# {enable | disable}]}
```

Syntax Description	
conn-max <i>number</i>	Sets the maximum number of simultaneous TCP and UDP connections, between 0 and 65535. The default is 0, which means no limit on connections.
conn-rate-limit <i>number</i>	Sets the maximum TCP and/or UDP connections per second between 0 and 65535. The default is 0, which means no limit on the connection rate.
disable	Turns off TCP sequence number randomization.
enable	Turns on TCP sequence number randomization.
random-seq#	Enables or disables TCP sequence number randomization. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The FWSM 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 FWSM, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You use a WAAS device that requires the FWSM not to randomize the sequence numbers of connections. Note Because of the way TCP sequence randomization is implemented, if you enable Xlate Bypass using the xlate-bypass command), then disabling TCP sequence randomization only works for control connections, and not data connections; for data connections, the TCP sequence continues to be randomized.

Defaults

For the **conn-max** keyword, the default value of *number* is 0, which allows unlimited connections.

For the **conn-rate-limit** keyword, the default value of *number* is 0, which allows unlimited connections per second.

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
3.1(1)	This command was introduced.
4.0(1)	The conn-rate-limit keyword was added. Also, when you match an access list in the class map, the set connection actions are performed for the access list as a whole instead of independently for each ACE.

Usage Guidelines

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **set connection** command to set connections for that class map.



Note

You can also configure maximum connections and TCP sequence randomization in the NAT configuration (the **nat** and **static** commands). If you configure these settings for the same traffic using both methods, then the FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

Unlike the **set connection** command, NAT also lets you configure embryonic connection limits, which triggers TCP Intercept to prevent a DoS attack.

Examples

The following example configures the maximum number of simultaneous connections as 256, the maximum rate as 50 per second, and disables TCP sequence number randomization:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 conn-rate-limit 50 random-seq#
disable
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.

service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.

set connection advanced-options tcp-state-bypass

To enable TCP state bypass, use the **set connection advanced-options** command in class configuration mode. The class configuration mode is accessible from the policy-map configuration mode. To disable TCP state bypass, use the **no** form of this command.

set connection advanced-options tcp-state-bypass

no set connection advanced-options tcp-state-bypass

Syntax Description

This command has no arguments or keywords.

Defaults

By default, TCP state bypass is disabled.

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
3.2(1)	This command was introduced.

Usage Guidelines

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **set connection advanced-options** command to enable TCP state bypass for that class map.

Allowing Outbound and Inbound Flows through Separate FWSMs

By default, all traffic that goes through the FWSM is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. The FWSM maximizes the firewall performance by checking the state of each packet (is this a new connection or an established connection?) and assigning it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection).

TCP packets that match existing connections in the fast path can pass through the FWSM without rechecking every aspect of the security policy. This feature maximizes performance. However, the method of establishing the session in the fast path using the SYN packet, and the checks that occur in the fast path (such as TCP sequence number), can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow of a connection must pass through the same FWSM.

For example, a new connection goes to FWSM 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through FWSM 1, then the packets will match the entry in the fast path, and are passed

through. But if subsequent packets go to FWSM 2, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped.

If you have asymmetric routing configured on upstream routers, and traffic alternates between two FWSMs, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet matching the specified networks enters the FWSM, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

Application Inspection Unsupported

Application inspection requires both inbound and outbound traffic to go through the same FWSM, so application inspection is not supported with TCP state bypass.

Trusted Flow Acceleration Unsupported

You cannot configure TCP state bypass and Trusted Flow Acceleration (the **set connection advanced-options service-acceleration** command) for the same traffic; unexpected behavior occurs.

Compatibility with NAT

Because the translation session is established separately for each FWSM, be sure to configure static NAT on both FWSMs for TCP state bypass traffic; if you use dynamic NAT, the address chosen for the session on FWSM 1 will differ from the address chosen for the session on FWSM 2.

Connection Timeout

If there is no traffic on a given connection for 2 minutes, the connection times out. You can override this default using the **set connection timeout tcp** command. Normal TCP connections timeout by default after 60 minutes.

Examples

The following is an example configuration for TCP state bypass:

```
hostname(config)# access-list tcp_extended permit tcp 10.1.1.0 255.255.255.0 10.2.1.0
255.255.255.0

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy outside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.

service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.

set connection timeout

To configure the timeout period after which an embryonic, half-closed, or idle connection is disconnected, 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] [half-closed hh:mm:ss] [tcp hh:mm:ss [reset]]] | idle hh:mm:ss]
```

```
no set connection timeout [[[embryonic hh:mm:ss] [half-closed hh:mm:ss] [tcp hh:mm:ss [reset]]] | idle hh:mm:ss]
```

Syntax Description

embryonic <i>hh:mm:ss</i>	Defines the timeout period until a TCP embryonic connection is closed, between 0:0:1 and 0:4:15. The default is 0:0:20. You can also set the value to 0, which means the connection never times out. Although you cannot set the maximum embryonic connections using the set connection command, you can set the timeout using this command.
half-closed <i>hh:mm:ss</i>	Defines the timeout period until a TCP half-closed connection is freed, between 0:0:1 and 0:4:15. The default is 0:0:20. You can also set the value to 0, which means the connection never times out.
idle <i>hh:mm:ss</i>	Defines the idle time after which an established connection of any protocol closes, between 0:5:0 and 1092:15:0. The default is 1:00:0. You can also set the value to 0, which means the connection never times out.
reset	(Optional) Sends a reset to TCP endpoints when the connection times out.
tcp <i>hh:mm:ss</i>	Defines the idle time after which a TCP established connection closes, between 0:5:0 and 1092:15:0. The default is 1:00:0. You can also set the value to 0, which means the connection never times out. This keyword has been replaced by the idle keyword, which applies to all protocols and not just to TCP. However, if you still have this command in your configuration, it is accepted. See the “ Usage Guidelines ” for more information about using both commands in the same policy.

Defaults

The default **embryonic** connection timeout value is 20 seconds.

The default **half-closed** connection timeout value is 20 seconds.

The default **idle** connection timeout value is 1 hour.

The default **tcp** connection timeout value is 1 hour.

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
3.1(1)	This command was introduced.
3.2(1)	Support for the idle keyword was introduced.

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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

You can enter the **tcp** keyword, **embryonic** keyword, and **half-closed** keyword together, however you must enter the **idle** keyword separately.

If you remove a timeout using the **no** form of the command, then all timeouts are removed. To change the value of a timeout, reenter the command with the new value instead of using the **no** form.

If you configure the **set connection timeout tcp** and **set connection timeout idle** commands for the same class, then the **idle** command (which sets the timeout for all types of connections) is used instead of the **tcp** command (which sets the timeout for TCP connections only) when the class map does not specifically match TCP traffic. If the class map matches an access list that specifies TCP traffic explicitly, then the **tcp** command is used instead of the **idle** command for TCP traffic; other traffic that matches the access list uses the **idle** command. The following example creates an access list with an ACE that specifically matches TCP traffic. Therefore, TCP traffic uses the **tcp** command, while UDP and ICMP traffic uses the **idle** command:

```
access-list ip_traffic extended permit tcp any any
access-list ip_traffic extended permit udp any any
access-list ip_traffic extended permit icmp any any
```

```
class-map c1
  match access-list ip_traffic
```

```
policy-map p1
  class c1
    set connection timeout idle 3:0:0
    set connection timeout tcp 2:0:0
```

```
service-policy p1 global
```

The following example has an access list that matches all IP traffic, and it does not specifically match TCP traffic. Therefore, even though the **tcp** command is present in the configuration, it is ignored in favor of the **idle** command for all traffic, including TCP traffic:

```
access-list ip_traffic extended permit ip any any
```

```
class-map c1
  match access-list ip_traffic
```

```
policy-map p1
  class c1
    set connection timeout idle 3:0:0
    set connection timeout tcp 2:0:0
```

```
service-policy p1 global
```

Examples

The following example sets the maximum TCP and UDP connections to 5000, and sets the maximum embryonic timeout to 40 seconds, the half-closed timeout to 20 minutes, and the idle timeout to 2 hours for traffic going to 10.1.1.1:

```
hostname(config)# access-list CONNS permit ip any host 10.1.1.1

hostname(config)# class-map conns
hostname(config-cmap)# match access-list CONNS

hostname(config-cmap)# policy-map conns
hostname(config-pmap)# class conns
hostname(config-pmap-c)# set connection conn-max 5000
hostname(config-pmap-c)# set connection timeout embryonic 0:0:40 half-closed 0:20:0
hostname(config-pmap-c)# set connection timeout idle 2:0:0

hostname(config-pmap-c)# service-policy conns interface outside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
set connection	Configures the maximum TCP and UDP connections.

set metric

To set the metric value for the destination 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 metric for the destination routing protocol, 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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 the FWSM through interactive prompts, enter the **setup** command in global configuration mode.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM requires some initial configuration before ASDM can connect to it. Before you enter the **setup** command, you must first name an interface “inside” with the **nameif** command. The FWSM does not have a default inside interface.

Once you enter the **setup** command, you are asked for the setup information in [Table 24-1](#).

Table 24-1 Setup Information

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 (<code>hostname(config)#</code>) appears.
Firewall Mode [Routed]:	Enter routed or transparent . The firewall mode prompt is available only in single mode or in a context.
Enable password:	Enter an enable password. (The password must have at least three characters.)
Inside IP address:	Enter the network interface IP address of the FWSM.

Table 24-1 Setup Information (continued)

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, 255.255.0.0, or 255.255.x.x. Use 0.0.0.0 to specify a default route. You can abbreviate the 0.0.0.0 netmask as 0.
Host name:	Enter the host name that you want to display in the command line prompt.
Domain name:	Enter the domain name of the network on which the FWSM runs.
IP address of host running Device Manager:	Enter the IP address on which ASDM connects to the FWSM.
Use this configuration and write to flash [yes]?	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.

The host and domain names are used to generate the default certificate for the Secure Socket Layer (SSL) connection.

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
Inside IP address [192.168.1.1]: 192.168.1.1
Inside network mask [255.255.255.0]: 255.255.255.0
Host name [tech_pubs]: tech_pubs
Domain name [your_company.com]: your_company.com
IP address of host running Device Manager:
```

The following configuration will be used:

```
Enable password: writer
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
```

Use this configuration and write to flash? **yes**

Related Commands

Command	Description
asdm	Configures the communication between the FWSM and a browser running the device manager.

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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines	If you omit the optional keyword locked, the FWSM 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      augry13
-          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 the 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.
<i>groupname</i>	(Optional) Shows statistics for servers in a group.
host <i>hostname</i>	(Optional) Shows statistics for a particular server in the group.
protocol <i>protocol</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support a LOCAL method.

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 FWSM 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 FWSM will communicate with this AAA server. - FAILED—The FWSM 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. You also see the date and time of the last transaction in the following form: Last transaction ({success failure}) at <i>time</i> <i>timezone</i> <i>date</i> If the FWSM 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.
Number of authentication requests	The number of authentication requests sent by the FWSM. This value does not include retransmissions after a timeout.

Field	Description
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 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 FWSM 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 FWSM 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 FWSM 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*] [**optimization** [**detail**] [**range** *low high*]]

Syntax Description	detail	Shows detailed access list optimization information.
	<i>id</i>	Identifies the access list.
	optimization	Shows access list optimization information.
	range <i>low high</i>	Shows the specified access list range.

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
	1.1(1)	This command was introduced.
	4.0(1)	Keywords optimization , detail , and range were added.

Usage Guidelines An ACL only denies SYN packets, so if another type of packet comes in, that packet will not show up in the access-list hit counters. TCP packet types other than SYN packets (including RST, SYN-ACK, ACK, PSF, and FIN) are dropped by the FWSM before they can be dropped by an access list. Only SYN packets can create a session in the Adaptive Security Algorithm, so only SYN packets are assessed by the access list.

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 hexadecimal identifier for each ACE at the end of each line.

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 commands in the configuration for features 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

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Usage Guidelines The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the FWSM Flash file system is the same as the activation key running on the FWSM, 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 FWSM Flash file system is different from the activation key running on the FWSM, 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 FWSM 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 oldkey, 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 FWSM uses the new 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
```

```
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
```

The flash activation key is the SAME as the running key.

```
hostname(config)#
```

Related Commands

Command	Description
activation-key	Changes the activation key.

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:

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

Command History

Release	Modification
2.2(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 disk:/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. This command shows dynamic and manual ARP entries, but does not identify the origin of each entry.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following is sample output from the **show arp** command:

```
hostname# show arp
  inside 10.86.195.205 0008.023b.9892
  inside 10.86.194.170 0001.023a.952d
  inside 10.86.194.172 0001.03cf.9e79
  inside 10.86.194.1  00b0.64ea.91a2
  inside 10.86.194.146 000b.fcf8.c4ad
  inside 10.86.194.168 000c.ce6f.9b7e
```

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:

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

Release	Modification
1.1(1)	This command was introduced.

Examples The following is sample output from the **show arp statistics** command:

```
hostname# show arp statistics
  Number of ARP entries:
  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 24-2 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 FWSM interfaces that were from the same IP address as that of a FWSM interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the FWSM 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 FWSM 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 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:

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

Command History	Release	Modification
	2.2(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 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 <i>feature</i>	(Optional) Limits the history display to the specified feature. The following are valid values for the <i>feature</i> 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 <i>if_name</i>—Displays the history for the specified interface. The <i>if_name</i> 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 <i>timeframe</i>	(Optional) Limits the history display to the specified time period. Valid values for the <i>timeframe</i> 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced (as show pdm history).
3.1(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:
```

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.

[illegible]

The following is sample output from the **show asdm history** command using the **snapshot** keyword:

```
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
```

show asdm history

```
HTTP Fixup Count:  [ 10s] : 0
FTP Fixup Count:   [ 10s] : 0
AAA Authentication Count: [ 10s] : 0
AAA Authorization 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 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:

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

Release	Modification
3.1(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 FWSM. 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show pdm sessions).
3.1(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 dropped packets or connections that take place in the control plane path, use the **show asp drop** command in privileged EXEC mode. This command only shows packet and flow drops for traffic that passes through the control plane path, including most inspected traffic, traffic destined directly to the FWSM, and all IPv6 traffic. Packets and flows that are processed and dropped in the FWSM hardware do not appear in the output.

show asp drop [**flow** *drop_reason* | **frame** *drop_reason*]

Syntax Description

flow	(Optional) Shows the dropped flows (connections).
frame	(Optional) Shows the dropped packets.
<i>drop_reason</i>	(Optional) Shows the flows or packets dropped by a particular process.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **show asp drop** command might help you troubleshoot a problem with the control plane. 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.

Related Commands

Command	Description
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 <i>ip_address</i>	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface <i>interface_name</i>	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask <i>mask</i>	(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:

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

Command History

Release	Modification
3.1(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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* 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
```

show asp table arp

```
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 [**crypto** | **domain** *domain_name* | **interface** *interface_name*]

Syntax Description

domain <i>domain_name</i>	(Optional) Shows entries for a specific classifier domain. See “ Usage Guidelines ” for a list of domains.
interface <i>interface_name</i>	(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* 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
```

■ show asp table classify

```
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
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
punt
punt-l2
punt-root
shun
tcp-intercept
```

Examples

The following is sample output from the **show asp table classify** command:

```
hostname# show asp table classify

Interface test:
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
...
```

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:

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

Release	Modification
3.1(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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* 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 301, 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 302, 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 303, 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 mac-address-table

To debug the accelerated security path MAC address tables, use the **show asp table mac-address-table** command in privileged EXEC mode.

show asp table mac-address-table [**interface** *interface_name*]

Syntax Description	interface (Optional) Shows MAC address tables for a specific interface. <i>interface_name</i>

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	—	•	•	•	•

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines	The show asp table mac-address-table command shows the MAC address table contents of the accelerated security path, which might help you troubleshoot a problem. See the <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide</i> 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 mac-address-table command:

```
hostname# show asp table mac-address-table
```

```
interface          mac    address          flags
-----
insidel            0009.b74d.3800   None
insidel            0007.e903.ad6e   None
insidel            0007.e950.2067   None
insidel            0050.0499.3749   None
insidel            0012.d96f.e200   None
insidel            0001.02a7.f4ec   None
insidel            0001.032c.6477   None
insidel            0004.5a2d.a1c8   None
insidel            0003.4773.c87b   None
```



```

inside1          000d.88ef.5d1c    None
inside1          00c0.b766.adce    None
inside1          0050.5640.450d    None
inside1          0001.03cf.0431    None
...

```

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

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 <i>ip_address</i>	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 <i>interface_name</i>	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask <i>mask</i>	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:

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

Command History

Release	Modification
3.1(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 *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* 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 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

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 <i>Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide</i> 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 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
...

```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asr

To display the members of ASR groups, use the **show asr** command in privileged EXEC mode.

show asr { *group_id* | **all** }

Syntax Description

<i>group_id</i>	Displays the VLANs that are members of the specified ASR group. Valid values are 1 through 32.
all	Displays the membership for all 32 ASR groups.

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
3.1(1)	This command was introduced.

Usage Guidelines

An ASR group can contain up to 8 members. A “0” (zero) in the output indicates an empty slot. The **show asr** command provides the same output as the **show np asr** command.

Examples

The following is sample output from the **show asr** command. It limits the display to VLANs that are members of ASR group 1.

```
hostname# sh asr 1
```

```
ASR Group | Vlan Entries in ASR Group (0 denotes empty slot)
-----|-----
      1 | 10  20  0  0  0  0  0  0  0
```

The following is sample output from the **show asr** command. It displays VLAN membership for all possible ASR groups. In this example, only ASR group 1 has member VLANs.

```
hostname# sh asr all
```

```
ASR Group | Vlan Entries in ASR Group (0 denotes empty slot)
-----|-----
      1 | 10  20  0  0  0  0  0  0  0
      2 |  0   0  0  0  0  0  0  0  0
      3 |  0   0  0  0  0  0  0  0  0
      4 |  0   0  0  0  0  0  0  0  0
```

```

 5 | 0 0 0 0 0 0 0 0 0
 6 | 0 0 0 0 0 0 0 0 0
 7 | 0 0 0 0 0 0 0 0 0
 8 | 0 0 0 0 0 0 0 0 0
 9 | 0 0 0 0 0 0 0 0 0
10 | 0 0 0 0 0 0 0 0 0
11 | 0 0 0 0 0 0 0 0 0
12 | 0 0 0 0 0 0 0 0 0
13 | 0 0 0 0 0 0 0 0 0
14 | 0 0 0 0 0 0 0 0 0
15 | 0 0 0 0 0 0 0 0 0
16 | 0 0 0 0 0 0 0 0 0
17 | 0 0 0 0 0 0 0 0 0
18 | 0 0 0 0 0 0 0 0 0
19 | 0 0 0 0 0 0 0 0 0
20 | 0 0 0 0 0 0 0 0 0
21 | 0 0 0 0 0 0 0 0 0
22 | 0 0 0 0 0 0 0 0 0
23 | 0 0 0 0 0 0 0 0 0
24 | 0 0 0 0 0 0 0 0 0
25 | 0 0 0 0 0 0 0 0 0
26 | 0 0 0 0 0 0 0 0 0
27 | 0 0 0 0 0 0 0 0 0
28 | 0 0 0 0 0 0 0 0 0
29 | 0 0 0 0 0 0 0 0 0
30 | 0 0 0 0 0 0 0 0 0
31 | 0 0 0 0 0 0 0 0 0
32 | 0 0 0 0 0 0 0 0 0

```

Related Commands

Command	Description
asr-group	Specifies an interface as a member of an ASR group.

show auto-update

To view the Auto Update Server configuration, use the **show auto-update** command in privileged EXEC mode.

show auto-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:

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

Release	Modification
3.1(1)	This command was introduced.

Examples The following is sample output from the **show auto-update** command:

```
hostname# show arp-inspection
Poll period: 1 minutes, retry count: 1, retry period: 5 minutes
Timeout: none
Device ID: host name [farscape]
```

Command	Description
auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the FWSM 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 FWSM if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration

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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	The pool summary option was added.

Usage Guidelines

The **show blocks** command helps you determine if the FWSM 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 FWSM. 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
    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 3](#) shows each field description.

Table 25-1 *show blocks Fields*

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type. Examples are shown below.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.
256	Used for Stateful Failover updates, syslogging, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active FWSM generates and sends packets to the standby FWSM 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 FWSM. 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 FWSM is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the FWSM is processing. Syslog messages sent out from the FWSM 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 FWSM configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

Table 25-1 *show blocks Fields (continued)*

Field	Description
1550	Used to store Ethernet packets for processing through the FWSM. When a packet enters a FWSM interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The FWSM 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 FWSM 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 FWSM attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the FWSM 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 FWSM 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 FWSM 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 4 shows each field description.

Table 25-2 *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.

Table 25-2 show blocks all Fields

Field	Description
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

```

show blocks

```

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 5 shows each field description.

Table 25-3 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 boot device (IOS)

To view the default boot partition, use the **show boot device** command.

show boot device [*mod_num*]

Syntax Description	<i>mod_num</i>	(Optional) Specifies the module number. Use the show module command to view installed modules and their numbers.

Defaults	The default boot partition is cf:4.

Command Modes	Privileged EXEC.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following is sample output from the **show boot device** command that shows the boot partitions for each installed FWSM on Cisco IOS software:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Related Commands	Command	Description
	boot device (IOS)	Sets the default boot partition.
	show module (IOS)	Shows all installed modules.

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

<i>capture_name</i>	(Optional) Name of the packet capture.
access-list <i>access_list_name</i>	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count <i>number</i>	(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 <i>number</i>	Starts the display at the specified packet number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
3.1(1)	Support for 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 25-4](#), the bracketed output is displayed when you specify the **detail** keyword.

Table 25-4 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	<i>HH:MM:SS.ms</i> [ether-hdr] <i>VLAN-info</i> <i>encap-ether-packet</i>
ARP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>arp-type</i> <i>arp-info</i>

Table 25-4 Packet Capture Output Formats (continued)

Packet Type	Capture Output Format
IP/ICMP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>ip-source</i> > <i>ip-destination</i> : icmp: <i>icmp-type icmp-code</i> [checksum-failure]
IP/UDP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr.src-port</i> <i>dest-addr.dst-port</i> : [checksum-info] udp <i>payload-len</i>
IP/TCP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr.src-port</i> <i>dest-addr.dst-port</i> : <i>tcp-flags</i> [header-check] [checksum-info] <i>sequence-number</i> <i>ack-number</i> <i>tcp-window</i> <i>urgent-info</i> <i>tcp-options</i>
IP/Other	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr</i> <i>dest-addr</i> : <i>ip-protocol</i> <i>ip-length</i>
Other	<i>HH:MM:SS.ms</i> <i>ether-hdr</i> : <i>hex-dump</i>

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 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1(1)	Support for 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:

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

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 FWSM Flash partition). The “.” shows that the FWSM 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:

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

Release	Modification
1.1(1)	This command was introduced.

Command History

Examples The following 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
```

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

Related Commands

show class

To show the contexts assigned to a class, use the **show class** command in privileged EXEC mode.

show class *name*

Syntax Description

<i>name</i>	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:

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

Command History

Release	Modification
2.2(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 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 [**all** | **count**] [**state** *state_type*] | [{ **foreign** | **local** } *ip* [-*ip2*] **netmask** *mask*] | [**long** | **detail**] | [{ {**lport** | **fport**} *port1* } [-*port2*]] | [**protocol** {**tcp** | **udp**}]

Syntax Description

all	Display connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
detail	Displays connections in detail, including translation type and interface information.
foreign	Displays connections with the specified foreign IP address.
fport	Displays connections with the specified foreign port.
<i>ip</i>	IP address in dotted-decimal format or beginning address in a range of IP addresses.
<i>-ip2</i>	(Optional) Ending IP address in a range of IP addresses.
local	Displays connections with the specified local IP address.
long	(Optional) Displays connections in long format.
lport	Displays connections with the specified local port.
netmask	Specifies a subnet mask for use with the given IP address.
<i>mask</i>	Subnet mask in dotted-decimal format.
<i>port1</i>	Port number or beginning port number in a range of port numbers.
<i>-port2</i>	(Optional) Ending port number in a range of port numbers.
protocol	(Optional) Specifies the connection protocol.
state	(Optional) Displays the state of specified connections.
<i>state_type</i>	Specifies the connection state type. See Table 7 for a list of the keywords available for connection state types.
tcp	Displays TCP protocol connections.
udp	Displays UDP protocol connections.

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
1.1(1)	This command was introduced.
3.2(1)	The b state for TCP state bypass and X state for xlate bypass were added.

Usage Guidelines

The **show conn** command displays the number of active TCP 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 FWSM 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 local** command.

The connection types that you can specify using the **show conn state** command are defined in [Table 7](#). When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 25-5 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.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.

When you use the **detail** option, the system displays information about the translation type and interface information using the connection flags defined in [Table 8](#).

Table 25-6 Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
b	State bypass
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	UDP 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
j	GTP data
J	GTP control
k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
n	GUP
N	Supervisor-based acceleration connection
O	outbound data
p	PISA connection
P	inside back connection
q	SQL*Net data
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection
R	UDP SunRPC ²
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection ³
T	SIP connection ⁴
U	up

Table 25-6 Connection Flags (continued)

Flag	Description
X	xlate creation bypassed
W	WAAS session

1. The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict inspections 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 FWSM 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 **conn timeout** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

Examples

When specifying multiple connection types, use commas without spaces to separate the keywords. The following is sample output including RPC, H.323, and SIP connection information in the Up state from the **show conn** command:

```
hostname# show conn state up,rpc,h323,sip
```

The following is sample output that shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 192.168.49.10. 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
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

The following sample output that shows a UDP connection from outside host 192.168.49.10 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(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
      B - initial SYN from outside, b - State bypass, 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 - Skinny media,
      M - SMTP data, m - SIP media, n - GUP, O - outbound data,
      P - inside back 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
      X - xlate creation bypassed
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

The following is sample output from a GRE session connection (PROT:47) from host 172.16.2.1 to host 172.16.112.2. Because it is a non TCP connection, it is unidirectional and there are no flags.

```
hostname# show conn
2 in use, 2 most used
Network Processor 1 connections
PROT:47 out 172.16.112.2 in 172.16.2.1 idle 0:00:08
Bytes 18
```

The following is sample output from the **show conn all** command:

```
hostname# show conn all
6 in use, 6 most used
TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

In this example, host 10.3.3.4 on the inside has accessed a website at 209.165.201.1. The global address on the outside interface is 209.165.201.7.

The following is sample output from the **show conn detail** command:

```
hostname# show conn detail
0 in use, 26152 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
      B - initial SYN from outside, b - State bypass, 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 - Skinny media,
      M - SMTP data, m - SIP media, n - GUP, O - outbound data,
      P - inside back 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
      X - xlate creation bypassed
Network Processor 1 connections
```

Related Commands

Commands	Description
inspect ctique	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. The FWSM automatically captures output destined for the internal console port. Do not use the internal console port unless you are advised to do so by Cisco TAC. This command allows you to view console output on your Telnet or SSH session.

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:

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines Information that displays only on a console port includes output from the **perfmom** command, startup messages, and some debug messages. The console buffer is a maximum of 1 K, and is not user configurable.

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
```

Command	Description
clear configure console	Restores the default console connection settings.

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.
<i>name</i>	(Optional) Sets the context name. If you do not specify a name, the FWSM displays all contexts. Within a context, you can only enter the current context name.

Defaults

In the system execution space, the FWSM 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:

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

Command History

Release	Modification
2.2(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 context** command. The following sample display shows three contexts:

```

Context Name      Class      Interfaces      Mode      URL
*admin            default    Vlan100,101     Routed     disk:/admin.cfg
contexta          Gold       Vlan200,201     Transparent disk:/contexta.cfg
contextb          Silver     Vlan300,301     Routed     disk:/contextb.cfg
Total active Security Contexts: 3

```

[Table 25-7](#) shows each field description.

Table 25-7 *show context Fields*

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Class	Shows the resource class to which the context belongs.
Interfaces	Shows the interfaces assigned to the context.
Mode	Shows the firewall mode for each context, either Routed or Transparent.
URL	Shows the URL from which the FWSM loads the context configuration.

The following is sample output from the **show context detail** command:

```
hostname# show context detail
```

```
Context "admin", has been created, but initial ACL rules not complete
```

```
Config URL: disk:/admin.cfg
```

```
Real Interfaces: Vlan100
```

```
Mapped Interfaces: Vlan100
```

```
Class: default, Flags: 0x00000013, ID: 1
```

```
Context "ctx", has been created, but initial ACL rules not complete
```

```
Config URL: disk:/ctx.cfg
```

```
Real Interfaces: Vlan10,20,30
```

```
Mapped Interfaces: int1, int2, int3
```

```
Class: default, Flags: 0x00000011, ID: 2
```

```
Context "system", is a system resource
```

```
Config URL: startup-config
```

```
Real Interfaces:
```

```
Mapped Interfaces: Vlan100,10,20,30
```

```
Class: default, Flags: 0x00000019, ID: 257
```

```
Context "null", is a system resource
```

```
Config URL: ... null ...
```

```
Real Interfaces:
```

```
Mapped Interfaces:
```

```
Class: default, Flags: 0x00000009, ID: 258
```

Table 25-8 shows each field description.

Table 25-8 *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 FWSM 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 FWSM 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.

Table 25-8 Context States

Field	Description
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 FWSM 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 FWSM 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 FWSM 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. The system execution space includes all interfaces.
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.
Class	The resource class to which the context belongs.
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.

Command	Description
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

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	(Multiple mode only) Displays counters for all contexts.
context <i>context-name</i>	(Multiple mode only) Specifies the context name for which to show counters.
:counter_name	Specifies a counter by name.
detail	Displays additional counter information.
protocol <i>protocol_name</i>	Displays the counters for the specified protocol.
summary	(Multiple mode only) Shows all context counters combined.
threshold <i>n</i>	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top <i>n</i>	(Multiple mode only) Shows the contexts that are the top <i>n</i> users of the specified counter. You must specify a counter name with this option. The range is 1 through 4294967295.

Defaults

For multiple context mode, the default context is **summary**, which shows counters for every context. For single mode, the context name is ignored and the output shows the “context” as “single_vf.”

The default count threshold is **1**.

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
2.2(1)	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      admin
IOS_IPC      OUT_PKTS       2      admin
IOS_IPC      IN_PKTS      15      customera
IOS_IPC      OUT_PKTS       6      customera
```

The following example shows how to display a summary of counters:

```
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 counters for a context:

```
hostname# show counters context admin
Protocol      Counter      Value      Context
IOS_IPC       IN_PKTS      4          admin
IOS_IPC       OUT_PKTS     4          admin
```

Related Commands

Command	Description
clear counters	Clears the protocol stack counters.
show counters description	Shows a list of protocol counters.

show counters description

To display the protocol stack counter descriptions, use the **show counters description** command in privileged EXEC mode.

show counters description

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	•	•	•	—	•

Release	Modification
2.2(1)	This command was introduced.

Examples The following is sample output from the **show counters description** command:

```
hostname# show counters description
Protocol      Counter      Description
NPCP          IN_PKTS      Packets from network processors
NPCP          OUT_PKTS     Packets to network processors
NPCP          DROP_LIMIT1  Gigamac packets dropped due to IP protocol que
ue limiter
NPCP          DROP_LIMIT2  Gigamac packets dropped due to ARP protocol qu
eue limiter
NPCP          DROP_LIMIT3  Gigamac packets dropped due to Fixup queue lim
iter
...
```

Related Commands	Command	Description
	clear counters	Clears the protocol stack counters.
	show counters	Shows 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 cpu threshold

To display the CPU usage information when the configured rising threshold is reached and remains for the configured monitoring interval period, use the **show cpu threshold** command in privileged EXEC mode.

show cpu threshold

Syntax Description This command has no keywords and no arguments.

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	•	•	•	•	•

Release	Modification
3.2(1)	This command was introduced.

Command History

Usage Guidelines The CPU usage threshold is computed using an approximation of the load for the configured monitoring period, and then by feeding this approximation into two moving averages.

Examples The following example shows how to display the CPU usage threshold:

```
hostname# show cpu threshold
CPU utilization RisingThresholdValue = 60%; RisingThresholdPeriod = 300secs
```

Command	Description
show cpu usage	Displays the CPU usage information.

Related Commands

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 FWSM 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:

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

Command History

Release	Modification
3.1	This command was introduced.

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 FWSM. 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	FragDBG
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 Collec
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	00f2bfbcb	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
Crđ	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):

```

show crashinfo

```

          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 FWSM.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the FWSM to save crash information to a file in Flash memory.

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:

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

Command History

Release	Modification
3.1(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 privileged EXEC mode.

show crypto ca certificates [*trustpointname*]

Syntax Description

trustpointname (Optional) Specifies 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CA certificate for a trustpoint named tp1:

```
hostname# 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.con
  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#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crt 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 privileged EXEC mode.

show crypto ca crls [*trustpointname*]

Syntax Description

trustpointname (Optional) Specifies 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CRL for a trustpoint named tp1:

```
hostname# 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
```

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 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

<i>interface</i>	Specifies an interface name.
<i>token</i>	Indicates 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show crypto ipsec .

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 modes.

show crypto ipsec fragmentation *interface*

Syntax Description

<i>interface</i>	Specifies an interface name.
token	Indicates a token-based server for user authentication is used.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show crypto ipsec .

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 key mypubkey

To display key pairs of the indicated type, use the **show crypto key mypubkey** command in privileged EXEC mode.

show crypto key mypubkey {rsa | dsa}

Syntax Description

dsa	Displays DSA key pairs.
rsa	Displays RSA key 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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, displays RSA key pairs:

```
hostname(config)# show crypto key mypubkey rsa
...
```

Related Commands

Command	Description
crypto key generate dsa	Generates DSA key pairs.
crypto key generate rsa	Generates RSA key pairs.
crypto key zeroize	Removes all key pairs of the indicated type.

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:

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

Command History

Release	Modification
3.1(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
```

show crypto protocol statistics

```

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 ctique

To display information about CTIQBE sessions established across the FWSM, use the **show ctique** command in privileged EXEC mode.

show ctique

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
	3.1(1)	This command was introduced.

Usage Guidelines The **show ctique** command displays information of CTIQBE sessions established across the FWSM. Along with **debug ctique** 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 ctique** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctique** command output to reach the end.

Examples

The following is sample output from the **show ctique** command under the following conditions. There is only one active CTIQBE session setup across the FWSM. 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 CallManager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
hostname# show ctique
```

```
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 FWSM 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

```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ctique	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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
```

 show curpriv

```
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

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 debug through show ipv6 traffic Commands

show debug

To show the current debugging configuration in privileged EXEC mode, 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 lets you 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The valid *command* values follow. For information about valid syntax after *command*, see the entry for **debug command**, as applicable.



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
- 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
- xdmcp

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 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.
<i>IP_address</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	This command was changed from show dhcprelay .

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.

Command	Description
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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	This command was changed from show dhcprelay .

Usage Guidelines The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples The following is 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
DHCPPOFFER       7
DHCPACK          3
DHCPNAK          0
FeralPix(config)#
```

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, use the **show disk** command in privileged EXEC mode.

show disk [filesystem | all]

Syntax Description	filesystem	Shows information about the compact Flash card.
	all	Shows the contents of Flash memory plus the file system information,

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
	2.2(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 fileys** command:

```

hostname# show disk fileys
***** 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

```

Related Commands

Command	Description
dir	Displays the directory contents.

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:

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

Command History	Release	Modification
	3.1(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 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
```

The **show dns-hosts** field descriptions are as follows:

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 FWSM 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 cache	Clears the DNS cache.
dns domain-lookup	Enables the FWSM 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 FWSM 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	<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
	<i>end</i>	(Optional) Limits the output to the entries with starting with the <i>start</i> index number and ending with the <i>end</i> index number.
	<i>start</i>	(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 <i>end</i> 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
	4.0(1)	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

<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are displaying active interfaces. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail information.
<i>if-name</i>	(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:

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

Command History

Release	Modification
4.0(1)	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
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes

show eigrp interfaces

```

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 26-1 describes the significant fields shown in the display.

Table 26-1 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 FWSM 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

<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail neighbor information.
<i>if-name</i>	(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
4.0(1)	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           Vlan10    13       0:00:41   0      11    4     20
```

■ show eigrp neighbors

```

172.16.80.28      Vlan10      14      0:02:01  0      10      12      24
172.16.80.31      Vlan10      12      0:02:02  0      4       5       20

```

Table 26-1 describes the significant fields shown in the display.

Table 26-2 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 FWSM receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the FWSM 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 FWSM considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the FWSM first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the FWSM 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 FWSM to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the FWSM 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 26-3 describes the significant fields shown in the display.

Table 26-3 show ip eigrp neighbors static Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Static Address	IP address of the EIGRP neighbor.
Interface	Interface on which the FWSM 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                 Vlan10 11 00:04:07 768   4608   0 4    S
    Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Vlan10 13 1w0d      1 3000   0 6    S
    Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                 Vlan10 12 1w0d      1 3000   0 4    S
    Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 26-4 describes the significant fields shown in the display.

Table 26-4 *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 FWSM receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the FWSM 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 FWSM considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the FWSM 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 FWSM to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the FWSM waits before resending a packet from the retransmission queue to a neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the FWSM 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.

Table 26-4 *show ip eigrp neighbors details Field Descriptions*

Field	Description
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.
<i>as-number</i>	(Optional)	Specifies the autonomous system number of the EIGRP process. Because the FWSM only supports one EIGRP routing process, you do not need to specify the autonomous system number.
<i>ip-addr</i>	(Optional)	The IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided.
<i>mask</i>	(Optional)	The network mask to apply to the <i>ip-addr</i> 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:

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

Command History	Release	Modification
	4.0(1)	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), Vlan10
    via 10.16.81.28 (46251776/46226176), Vlan10
P 10.16.81.0 255.255.255.0, 1 successors, FD is 307200
    via Connected, Vlan1
    via 10.16.81.28 (307200/281600), Vlan10
    via 10.16.80.28 (307200/281600), Vlan10
```

Table 26-5 describes the significant fields shown in the displays.

Table 26-5 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 <i>n</i> of these entries, where <i>n</i> 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 (Vlan10), 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 (Vlan10), 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	<i>as-number</i>	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the FWSM 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:

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

Command History	Release	Modification
	4.0(1)	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 26-3 describes the significant fields shown in the display.

Table 26-6 *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.
interface	Displays failover command and stateful link information.
<i>num</i>	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, if a unit is in the failed state, the reason for the failure.
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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.1(1)	Support for the Autostate feature and suspend configuration synchronization were added.
3.1(1)	This command was modified to include failover groups. 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.

In the **show failover** command output, the 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 FWSM up time, which the active FWSM passes on to the standby FWSM.
 - 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.

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.

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.

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan 101 (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)
    Interface inside (10.130.9.3): Normal
    Interface outside (10.132.9.3): Normal
  Other host: Secondary - Standby Ready
    Active time: 0 (sec)
    Interface inside (10.130.9.4): Normal
    Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
Link : fover Vlan 101 (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

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 Vlan 101(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)

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)

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 Vlan 101 (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

Logical Update Queue Information
          Cur      Max      Total
Recv Q:   0        1      1895
Xmit Q:   0        0      1940

```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the current configuration.

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.
	<i>filename</i>	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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History	Release	Modification
	3.1(1)	Support for 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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	In the system execution space, this command now shows the firewall mode for each context. You can now set the firewall mode independently for each context.

Examples The following is sample output from the **show firewall** command in single mode or within a context:

```
hostname# show firewall
Firewall mode: Router
```

The following is sample output from the **show firewall** command within a context:

```
hostname# show firewall

Context      Mode
-----
customerA    Transparent
customerB    Routed
```

Related Commands	Command	Description
	firewall transparent	Sets the firewall mode.
	show mode	Shows the current context mode, either single or multiple.

show firewall autostate (IOS)

To view the setting of the autostate feature, use the **show firewall autostate** command in privileged EXEC mode. Autostate messaging in Cisco IOS software allows the FWSM to quickly detect that a switch interface has failed or come up.

show firewall autostate

Syntax Description	This command has no arguments or keywords.

Defaults	By default, autostate is disabled.

Command Modes	Privileged EXEC.

Command History	Release	Modification
	12.2(18)SXF5	This command was introduced.

Usage Guidelines	The switch supervisor sends an autostate message to the FWSM when:
	• The last interface belonging to a VLAN goes down. • The first interface belonging to a VLAN comes up.

Related Commands	Command	Description
	firewall autostate	Enables the autostate feature.

show firewall module (IOS)

To view the VLAN groups assigned to each FWSM, enter the **show firewall module** command in privileged EXEC mode.

show firewall module [*module_number*]

Syntax Description	<i>module_number</i>	(Optional) Specifies the module number. Use the show module command to view installed modules and their numbers.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC mode.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following is sample output from the **show firewall module** command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands	Command	Description
	firewall module	Assigns a VLAN group to an FWSM.
	firewall vlan-group	Assigns VLANs to a VLAN group.
	show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
	show module	Shows all installed modules.

show firewall vlan-group (IOS)

To view VLAN groups that can be assigned to the FWSM, enter the **show firewall vlan-group** command in privileged EXEC mode.

show firewall vlan-group [*firewall_group*]

Syntax Description	<i>firewall_group</i> (Optional) Specifies the group ID.

Defaults	No default behavior or values.

Command Modes	Privileged EXEC mode.

Command History	Release	Modification
	Preexisting	This command was preexisting.

Examples The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
-----
 50 55-57
 51 70-85
 52 100
```

Related Commands	Command	Description
	firewall module	Assigns a VLAN group to an FWSM.
	firewall vlan-group	Creates a group of VLANs.
	show module	Shows all installed modules.

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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(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.
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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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 FWSM, 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:

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines The **show h225** command displays information for H.225 sessions established across the FWSM. 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 FWSM 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 that 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 FWSM by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
timeout	Configures the idle timeouts related to H.225 and H.323.

show h245

To display information for H.245 sessions established across the FWSM 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:

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines The **show h245** command displays information for H.245 sessions established across the FWSM 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 FWSM. 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 FWSM by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
timeout	Configures the idle timeouts related to H.225 and H.323.

show h323

To display information for H.323 RAS or GUP sessions established across the FWSM between a gatekeeper and its H.323 endpoint, use the **show h323** command in privileged EXEC mode.

show h323 [gup | ras]

Syntax Description

gup	Displays the GUP session information.
ras	Displays the RAS session information.

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
3.2(1)	This command was introduced.

Usage Guidelines

The **show h323** command displays information for H.323 RAS or GUP sessions established across the FWSM 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** 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** command:

```
hostname# show h323 gup
No   Local                Foreign
1    inside:100.0.0.7/8549outside:100.0.0.6/35510
```

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 FWSM by endpoints using slow start.

Commands	Description
show h323-ras	Displays information for H.323 RAS sessions established across the FWSM.
timeout	Configures the idle timeouts related to H.225 and H.323.

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:

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

Release	Modification
Preexisting	This command was preexisting.

Command History

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 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:

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

Release	Modification
3.1(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 16464. In use 14.

              HWIDBs      SWIDBs
              Active 3      13
              Inactive 1      1
              Total IDBs 4      14
Size each (bytes) 156      260
Total bytes 624      3640

HWIDB# 1 0x2e63b40 EOBC
HWIDB# 2 0x2e4fd00 Vlan
HWIDB# 3 0x2e5f670 Vlan

SWIDB# 1 0x02e4fdc8 0xffffffff Vlan UP UP
SWIDB# 2 0x04b97970 0xffffffff Vlan20 UP UP
SWIDB# 3 0x04b98c58 0xffffffff Vlan22 UP UP
SWIDB# 4 0x04b98e48 0xffffffff Vlan34 UP UP
SWIDB# 5 0x04b99038 0xffffffff Vlan35 UP UP
SWIDB# 6 0x04b99228 0xffffffff Vlan36 UP UP

```



```

SWIDB# 7 0x04b99418 0xffffffff Vlan37 UP UP
SWIDB# 8 0x04b99608 0xffffffff Vlan38 UP UP
SWIDB# 9 0x04b997f8 0xffffffff Vlan124 UP UP
SWIDB# 10 0x04b999f8 0xffffffff Vlan136 UP UP
SWIDB# 11 0x04b99bf8 0xffffffff Vlan137 UP UP
SWIDB# 12 0x02e5f738 0xffffffff Vlan UP UP
SWIDB# 13 0x02e63c08 0x00000103 EOBC UP UP

```

Fields and description are as follows:

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 interface 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 FWSM 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.
<i>group</i>	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
<i>if_name</i>	(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:

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

Command History

Release	Modification
3.1(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	<i>if_name</i> (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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines	If you omit the optional <i>if_name</i> 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 FWSM 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:

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

Command History	Release	Modification
	3.1(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

Valid IGMP Packets      Received      Sent
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	Clears the IGMP traffic counters.

show interface

To display the information about the VLAN configuration, use the **show interface** command in privileged EXEC mode.

show interface [*interface_name*] [**detail** | **stats** | {**ip** [**brief**] }]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
detail	(Optional) Displays the interface configuration details.
stats	(Optional) Displays the interface statistics.
ip	(Default) Displays information about the interface IP configuration.
brief	(Optional) Displays compacted information about the interface IP configuration.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to include the new interface numbering scheme, and to add the stats keyword for clarity, and the detail keyword.

Usage Guidelines

You can use this command to display the status of interfaces. You can specify the ID (as either the VLAN or the mapped name) or the name of the interface.

The dropped packets statistic in the display shows a record of those packets that arrived on the interface, but were not destined for the FWSM. These packets include traffic flooded by the switch, multicast and broadcast traffic (unless the FWSM is configured to relay those) and packets that fail sanity checks such as incorrect IP length versus Layer 2 length or checksums. This counter does not record packets dropped by the security policy.

Examples

The following is sample output from the **show interface** command:

```
hostname# show interface
Interface Vlan20 "outsidedmz", is down, line protocol is down
      MAC address 000f.90d7.1a00, MTU 1500
```

```

        IP address 10.0.0.1, subnet mask 255.0.0.0
Traffic Statistics for "outsidedmz":
    0 packets input, 0 bytes
    0 packets output, 0 bytes
    0 packets dropped
Interface Vlan55 "inside", is up, line protocol is up
    MAC address 000f.90d7.1a00, MTU 1500
    IP address 192.168.62.20, subnet mask 255.255.255.0
Traffic Statistics for "inside":
    14582034 packets input, 2171077656 bytes
    406297 packets output, 243028833 bytes
    14812043 packets dropped
Interface Vlan56 "outside", is up, line protocol is up
    MAC address 000f.90d7.1a00, MTU 1500
    IP address 10.1.1.1, subnet mask 255.0.0.0
Traffic Statistics for "outside":
    0 packets input, 0 bytes
    33 packets output, 2244 bytes
    569730 packets dropped
Interface Vlan80 "", is up, line protocol is up
    Available but not configured via nameif

```

Field descriptions for the **show interface** command are shown below:

Field	Description
Interface <i>ID</i>	The interface ID. Within a context, the FWSM shows the mapped name (if configured), unless you set the allocate-interface command visible keyword.
<i>"interface_name"</i>	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
<i>is state</i>	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 <i>state</i>	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.
<i>message area</i>	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
MAC address	The interface MAC address.
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."

Field	Description
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.
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.

The following is sample output from the **show interface detail** command:

```
hostname# show interface detail
Interface Vlan20 "outsidedmz", is down, line protocol is down
    MAC address 000f.90d7.1a00, MTU 1500
    IP address 10.0.0.1, subnet mask 255.0.0.0
    Traffic Statistics for "outsidedmz":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
    Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is not active
    Control Point Vlan20 States:
        Interface vlan config status is not active
        Interface vlan state is UP
Interface Vlan55 "inside", is up, line protocol is up
    MAC address 000f.90d7.1a00, MTU 1500
    IP address 172.23.62.20, subnet mask 255.255.255.0
    Traffic Statistics for "inside":
        14582811 packets input, 2171191886 bytes
        406469 packets output, 243041933 bytes
        14812823 packets dropped
    Control Point Interface States:
        Interface number is 2
        Interface config status is active
        Interface state is active
    Control Point Vlan55 States:
        Interface vlan config status is active
        Interface vlan state is UP
Interface Vlan56 "outside", is up, line protocol is up
    MAC address 000f.90d7.1a00, MTU 1500
    IP address 1.1.1.1, subnet mask 255.0.0.0
    Traffic Statistics for "outside":
        0 packets input, 0 bytes
        33 packets output, 2244 bytes
        570042 packets dropped
    Control Point Interface States:
        Interface number is 3
        Interface config status is active
        Interface state is active
    Control Point Vlan56 States:
        Interface vlan config status is active
        Interface vlan state is UP
Asymmetrical Routing Statistics:
    Received 0 packets
```

```

Transmitted 163 packets
Dropped 0 packets
Interface Vlan80 "", is up, line protocol is up
Available but not configured via nameif

```

Each field description for the **show interface detail** command is shown below.

Field	Description
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 FWSM brings the interfaces up or down as needed.
Control Point <i>vlan</i> States:	
Interface vlan 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 vlan 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 FWSM 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.
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 [*interface interface_name*] **ip brief**

Syntax Description

interface <i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
ip brief	(Optional) Displays compacted information about the interface IP configuration.

Defaults

If you do not specify an interface, the FWSM shows all interfaces.

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
3.1(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.

Examples

The following is sample output from the **show ip brief** command:

```
hostname# show interface ip brief
Interface          IP-Address      OK? Method  Status        Protocol
Vlan10 209.165.200.226 YES CONFIG up            up
Vlan40 unassigned    YES unset    administratively down down
Vlan41 10.1.1.50      YES manual  administratively down down
Vlan42 192.168.2.6     YES DHCP    administratively down down
```

The field descriptions for the **show interface ip brief** command are as follows:

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the allocate-interface command.
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 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 [**interface** *interface_name*]

Syntax Description

interface *interface_name* (Optional) Shows statistics for the specified interface.

Defaults

If you do not specify an interface, the FWSM shows all interface IP addresses.

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
1.1(1)	This command was introduced.

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
Vlan20         mgmt      10.7.12.100     255.255.255.0    CONFIG
Vlan22         inside    10.1.1.100      255.255.255.0    CONFIG
Vlan34         outside   209.165.201.2   255.255.255.224  DHCP
Vlan35         dmz       209.165.200.225 255.255.255.224  manual

Current IP Addresses:
Interface      Name      IP address      Subnet mask      Method
Vlan36         mgmt      10.7.12.100     255.255.255.0    CONFIG
Vlan37         inside    10.1.1.100      255.255.255.0    CONFIG
Vlan38         outside   209.165.201.2   255.255.255.224  DHCP
Vlan124        dmz       209.165.200.225 255.255.255.224  manual
```

The current IP addresses are the same as the system IP addresses on the failover active module. When the primary module fails, the current IP addresses become the IP addresses of the standby module.

The field descriptions for the **show ip address** command are as follows:

Field	Description
Interface	The interface ID.
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 bgp neighbors

To display information about the TCP and BGP connections to neighbors, use the **show ip bgp neighbors** command in privileged EXEC mode.

show ip bgp 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History	Release	Modification
	3.2(1)	This command was introduced.

Usage Guidelines Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples The following is sample output from the **show ip bgp neighbors** command.

```
hostname# show ip bgp neighbors
```

```
BGP neighbor is 10.6.20.10, remote AS 100, internal link
  BGP version 4, remote router ID 120.1.1.1
  BGP state = Established, up for 00:09:18
  Last read 00:00:20, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                                Sent          Rcvd
```

■ show ip bgp neighbors

```

Opens:          1          1
Notifications:  0          0
Updates:        1          0
Keepalives:     12         11
Route Refresh:  0          0
Total:          14         13
Default minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast
neighbor version 1
Index 0, Offset 0, Mask 0x0

Prefix activity:
Sent      Rcvd
----
Prefixes Current:  0      0
Prefixes Total:    0      0
Implicit Withdraw:  0      0
Explicit Withdraw:  0      0
Used as bestpath:  n/a    0
Used as multipath:  n/a    0
Number of NLRI's in the update sent: max 1, min 0

Connections established 1; dropped 0
Last reset never

```

Table 26-7 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are displayed only when the counter has a non-zero value.

Table 26-7 The show ip bgp neighbors Command Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous-system number of the neighbor.
internal link	“internal link” is displayed for iBGP neighbors. “external link” is displayed for eBGP neighbors. For BGP stub routing, only iBGP is supported.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in seconds, that the underlying TCP connection has been in existence.
Last read	Time since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
keepalive interval	Time, interval in seconds, that keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers.
Route Refresh	Status of the route refresh capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.

Table 26-7 The show ip bgp neighbors Command Field Descriptions (continued)

Field	Description
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Received	Total number of received messages.
Opens	Number of open messages sent and received.
notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family for which the following fields refer.
neighbor version	Number used by Cisco IOS to track prefixes that have been sent and those that need to be sent.
Prefix activity	Prefix statistics for this address family.
Prefixes current	Number of prefixes accepted for this address family.
Prefixes total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that prefix is withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as a best paths.
Used as multipath	Number of received prefixes installed as multipaths.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection have been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.

Related Commands

Command	Description
neighbor	Specifies the BGP neighbor.
router bgp	Creates a BGP routing process and enters router configuration mode for that process.
show running-config router	Displays the router commands in the running configuration.

show ip bgp neighbors advertised-routes

To display the routes that are advertised to the BGP neighbor, use the **show ip bgp neighbors advertised-routes** command in privileged EXEC mode.

show ip bgp neighbors advertised-routes

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 ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History	Release	Modification
	3.2(1)	This command was introduced.

Usage Guidelines In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples The following example displays routes advertised for the BGP neighbor:

```
hostname# show ip bgp neighbors advertised-routes

local router ID is 5.6.7.8
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*  171.0.0.0/8      10.6.37.124             0   100 32768  i
```

[Table 26-8](#) describes the fields shown in the display.

Table 26-8 *The show ip bgp neighbors advertised-routes Field Information*

Field	Description
local router ID	The router ID of the FWSM. In order of precedence and availability, the router ID specified by the bgp router-id command or the highest IP address.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened and will not be advertised to BGP neighbors. h—The table entry does not contain the best path based on historical information. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an iBGP session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from IGP and was advertised with a network router configuration command. e—Entry originated from EGP. ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands	Command	Description
	network	Defines the networks that can be advertised by the BGP routing process.
	router bgp	Creates a BGP routing process and enters router configuration mode for that process.

show ip bgp summary

To display the status of the BGP connection, use the **show ip bgp summary** command in privileged EXEC mode.

show ip bgp 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context ¹	System
Privileged EXEC	•	—	•	•	—

1. This command is only available in the admin context.

Command History	Release	Modification
	3.2(1)	This command was introduced.

Usage Guidelines In multiple context mode, this command is only available in the admin context. The admin context must be in routed mode. The BGP stub routing configuration entered in the admin context applies to all contexts configured on the device; you cannot configure BGP stub routing on a per-context basis.

Examples The following is sample output from the **show ip bgp summary** command.

```
hostname# show ip bgp summary
```

```
BGP router identifier 5.6.7.8, local AS number 100
```

```
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
10.6.20.10 4  100    7        8        1     0    0   00:03:50 (NoNeg)
```

Table 26-9 describes the significant fields shown in the display. Fields that are preceded by the asterisk character are not shown in the preceding output.

Table 26-9 The show ip bgp summary Command Field Descriptions

Field	Description
BGP router identifier	In order of precedence and availability, the router identifier specified by the bgp router-id command or the highest IP address.
local AS number	The autonomous system number of the FWSM.
Neighbor	IP address of the neighbor.
V	BGP version number spoken to the neighbor.
AS	Autonomous system number.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Last version of the BGP database that was sent to the neighbor.
InQ	Number of messages queued to be processed from the neighbor.
OutQ	Number of messages queued to be sent to the neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor.

Related Commands

Command	Description
neighbor	Specifies the BGP neighbor.
network	Specifies the networks that can be advertised by the BGP routing process.
router bgp	Creates a BGP routing process and enters router configuration mode for that process.
show running-config router	Displays the router commands in the running configuration.

show ip nbar protocol-tagging (IOS)

If you use Programmable Intelligent Services Accelerator (PISA) integration with the FWSM, then to view , use the **show ip nbar protocol-tagging** command in privileged EXEC mode.



Note

This feature depends on Cisco IOS Release 12.2(18)ZYA, and will not be supported on the FWSM until the Cisco IOS software is released.

show ip nbar protocol-tagging {key | interface *ifname* | summary}

Syntax Description

key	Shows the GRE key used to tag the packets.
interface <i>ifname</i>	Shows if tagging is enabled on an interface.
summary	Shows a summary of the protocol tagging configuration.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.2(18)ZYA	This command was introduced.

Examples

The following is sample output from the **show ip nbar protocol-tagging summary** command:

```
Router# show ip nbar protocol-tagging summary
NBAR Tagging key:  0xFEEFABBA(default)
NBAR Tagging is enabled on the following interfaces:
  FastEthernet2/12
```

The following is sample output from the **show ip nbar protocol-tagging key** command:

```
Router# show ip nbar protocol-tagging key
NBAR Tagging key:  0xFEEFABBA(default)
```

The following is sample output from the **show ip nbar protocol-tagging interface** command:

```
Router# show ip nbar protocol-tagging interface FastEthernet 2/12
NBAR Tagging is enabled on this interface.
  vlan-list: 3,5,7-10
```

Related Commands

Command	Description
ip nbar protocol-tagging (IOS)	Enables protocol tagging.

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 <i>interface_name</i> (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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced,

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 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 <i>map-name</i>	(Optional) Displays IPsec SAs for the specified crypto map.
peer <i>peer-addr</i>	(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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
  #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)#

```

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): (10.132.0.21/255.255.255.0/0/0)
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): (10.132.0.21/255.255.255.0/0/0)
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): (10.132.0.21/255.255.255.0/0)
        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): (10.132.0.21/255.255.255.0/0)
        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 FWSM.
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:

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

Command History

Release	Modification
3.1(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:

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

Command History	Release	Modification
	3.1(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
```

```
Outbound
```

```
  Bytes: 4441740
```

```
  Uncompressed bytes: 4441740
```

```
  Packets: 74029
```

```
  Dropped packets: 0
```

```
  Authentications: 74029
```

```
  Authentication failures: 0
```



```
Encryptions: 74029
Encryption failures: 0
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 FWSM.

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 <i>source-ipv6-address</i>	(Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed.
<i>id</i>	(Optional) The access list name. When provided, only the specified access list is displayed.
<i>source-ipv6-prefix</i> <i>/prefix-length</i>	(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:

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

Command History

Release	Modification
3.1(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.
<i>if_name</i>	(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:

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

Command History

Release	Modification
3.1(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 Vlan101 "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):
    FE02::1
    FE02::1:FE11:6770
  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 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

<i>address</i>	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
<i>if_name</i>	(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:

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

Command History

Release	Modification
3.1(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:

- **INCOMP**—(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:

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

Release	Modification
3.1(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:

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

Command History

Release	Modification
3.1(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:

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

Command History	Release	Modification
	3.1(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
  unreachable: 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
```

■ show ipv6 traffic

```

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 sa through show route Commands

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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

Usage Guidelines	The output from this command includes the following fields: Detail not specified.

Table 27-1

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

Table 27-2

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
hostname(config)# sho 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 FWSM.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in 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:

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

Release	Modification
3.1(1)	This command was introduced.

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.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM.
show running-config isakmp	Displays all the active ISAKMP configuration.

show local-host

To display the IP addresses of hosts that initiated current connections through the FWSM, use the **show local-host** command in privileged EXEC mode. This command also shows the address translation, if present, and the number of TCP, UDP, and embryonic connections per host.

show local-host [*ip_address*] [**detail**] [**all**]

Syntax Description

all	(Optional) Shows all initiating hosts, including connections to or from the FWSM. If you do not use the all keyword, connections to the FWSM and from the FWSM do not display.
detail	(Optional) Displays detailed network states.
<i>ip_address</i>	(Optional) Specifies the initiating host IP address.

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
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
2.3(1)	Because the TCP intercept feature was changed to use SYN cookies, this command no longer shows embryonic connections above the embryonic connection limit.

Usage Guidelines

In most cases, the “local host” is the initiating host. However, if you configure static NAT for an IP address, that host always shows as the local host even if they did not initiate the connection.

If you configure outside NAT (either static NAT or NAT exemption), and an inside host initiates a connection to the outside host, both the inside and outside hosts are listed as local hosts in the **show local-host** output. This feature lets you track connection limits for both hosts.

If you configure an embryonic connection limit, and the limit is exceeded, the FWSM implements TCP intercept to prevent a SYN attack. After TCP intercept is triggered, additional embryonic connections do not appear in the **show local-host** output.

The connection limits are set using the **nat** or **static** commands, or using the **set connection** commands.

Examples

The following examples show how to display the network states of local hosts:

```
hostname# show local-host
local host: <10.5.59.30>, tcp conn(s)/limit = 1/0, embryonic(s)/limit =
0/0 udp conn(s)/limit = 0/0
  Xlate(s):
    Global 10.5.59.30 Local 10.5.59.30
```

Table 27-3 show local-host Fields

Field	Description
local host: <ip_address>	Shows the host IP address.
tcp conn(s)/limit = x/y	Shows the current TCP connections followed by the connection limit. 0 means no limit was set.
embryonic(s)/limit = x/y	Shows the current embryonic connections followed by the connection limit. 0 means no limit was set.
udp conn(s)/limit = x/y	Shows the current UDP connections followed by the connection limit. 0 means no limit was set.
Xlate(s):	Shows the address translation. The FWSM shows the same address for local and global if you did not configure NAT, or if you configured identity NAT or NAT exemption.

Related Commands

Command	Description
clear local-host	Clears connections.
nat	Associates a network with a pool of global IP addresses.
show conns	Shows connection information.
static	Statically translates an address.
set connection	Sets connection limits.

show logging

To show syslogs currently in the log buffer or to show other logging settings, use the **show logging** command in privileged EXEC mode.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

Syntax Description

message	(Optional) Displays messages that are at a non-default level. See the logging message command to set the message level.
<i>syslog_id</i>	(Optional) Specifies a message number to display.
all	(Optional) Displays all syslog IDs, along with whether they are enabled or disabled.
setting	(Optional) Displays the logging setting, without displaying the logging buffer.
asdm	(Optional) Displays ASDM logging buffer content.
queue	(Optional) Displays messages currently in the logging queue.

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.

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 lets 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

Examples

The following is sample 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 is sample 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 message	Sets the message level, or disables messages.
logging queue	Configures the logging queue.

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.
	<i>interface_name</i>	(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:

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

Release	Modification
2.2(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:

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

Release	Modification
3.1	This command was introduced.

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
```

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the FWSM.
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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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.

You can also display the information from the **show memory** command using SNMP.

Examples

The following 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: 15958088 bytes (24%)
Used memory:
Allocated memory in use: 29680332 bytes (44%)
Reserved memory: 21470444 bytes (32%)
-----
```

```

Total memory: 67108864 bytes (100%)

Least free memory: 4551716 bytes ( 7%)
Most used memory: 62557148 bytes (93%)

----- fragmented memory statistics -----

fragment size count total
(bytes) (bytes)
-----
16 8 128
24 4 96
32 2 64
40 5 200
64 3 192
88 1 88
168 1 168
224 1 224
256 1 256
296 2 592
392 1 392
400 1 400
1816 1 1816*
4435968 1 4435968**
11517504 1 11517504

* - top most releasable chunk.
** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size count total
(bytes) (bytes)
-----
40 50 2000
48 144 6912
56 24957 1397592
64 101 6464
72 99 7128
80 1032 82560
88 18 1584
96 64 6144
104 57 5928
112 6 672
120 112 13440
128 15 1920
136 87 11832
144 22 3168
152 31 4712
160 90 14400
168 65 10920
176 74 13024
184 11 2024
192 8 1536
200 1 200
<output omitted>

```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the FWSM.
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:

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

Command History

Release	Modification
3.1(1)	Support for 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 FWSM.
show memory profile	Displays information about the memory usage (profiling) of the FWSM.
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:

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

Release	Modification
3.1(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 27-4 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 27-4 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 FWSM, 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
3.1(1)	Support for 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 FWSM might experience a temporary reduction in performance when memory profiling is enabled

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 hexadecimal 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 held:

```
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).

Command	Description
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-caller address

To display the address ranges configured on the FWSM, 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:

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

Release	Modification
3.1(1)	Support for 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:
```

■ show memory-caller address

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 privileged EXEC mode.

show mfib [*group* [*source*]] [**verbose**]

Syntax Description

<i>group</i>	(Optional) IP address of the multicast group.
<i>source</i>	(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:

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

Command History

Release	Modification
3.1(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 privileged EXEC mode.

show mfib [*group*] **active** [*kbps*]

Syntax Description

<i>group</i>	(Optional) IP address of the multicast group.
<i>kbps</i>	(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:

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

Command History

Release	Modification
3.1(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 FWSM 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 privileged EXEC mode.

```
show mfib [group [source]] count
```

Syntax Description

<i>group</i>	(Optional) IP address of the multicast group.
<i>source</i>	(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:

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

Command History

Release	Modification
3.1(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 privileged EXEC mode.

show mfib interface *[interface]*

Syntax Description	<i>interface</i> (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:

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

Command History	Release	Modification
	3.1(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]
Vlan101             up          [no, no]
Vlan102             up          [no, no]
Vlan103             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 privileged EXEC mode.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

Syntax Description	active	(Optional) Displays active multicast sources.
	count	(Optional) Displays packet and route count data.
	<i>kpbs</i>	(Optional) Limits the display to active multicast sources greater-than or equal to this value.
	verbose	(Optional) Displays additional information.

Defaults The default value for *kpbs* is 4.

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

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

Command History	Release	Modification
	3.1(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 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:

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

Release	Modification
3.1(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
```

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 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:

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

Command History

Release	Modification
3.1(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 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:

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

Release	Modification
3.1(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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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# 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
```

show mgcp

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

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
```

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 mode

To show the security context mode, 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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.

Examples The following is sample output from the **show mode** command.

```
hostname# show mode
Firewall mode: multiple
The flash mode is the SAME as the running mode.
```

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 mrib client

To display information about the MRIB client connections, use the **show mrib client** command in 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:

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

Command History	Release	Modification
	3.1(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 privileged EXEC mode.

show mrib route *[[source | *] [group[/prefix-length]]]*

Syntax Description

<i>*</i>	(Optional) Display shared tree entries.
<i>/prefix-length</i>	(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.
<i>group</i>	(Optional) IP address or name of the group.
<i>source</i>	(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:

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

Command History

Release	Modification
3.1(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 mrrib route summary	Displays a summary of the MRIB table entries.

show mrrib route summary

To display a summary of the MRIB table entries, use the **show mrrib route summary** command in privileged EXEC mode.

show mrrib route 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples The following is sample output from the **show mrrib route summary** command:

```
hostname# show mrrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 0
```

Related Commands

Command	Description
show mrrib route	Displays 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 <i>rate</i>	(Optional) Displays only active multicast sources. Active sources are those sending at the specified <i>rate</i> or higher. If the <i>rate</i> 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.
	<i>source</i>	(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **show mroute** command displays the contents of the multicast routing table. The FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 FWSM 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 nameif

To view the interface name set using the **nameif** command, use the show nameif command in privileged EXEC mode.

```
show nameif [mapped_name]
```

Syntax Description	mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.

Defaults	If you do not specify an interface, the FWSM shows all interface names.	

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
	1.1(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 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
Vlan20 outside      0
Vlan35 inside        100
Vlan36 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 np

To display information about the network processors, use the **show np** command in privileged EXEC mode.

```
show np {number item | all}
```

Syntax Description

show np	Shows the maximum and free s in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.
number	The network processor number, in single digit format. You can enter 1, 2, or 3.
item	Use the following values to display information about the corresponding item: arp—Show arp information asr-table—Show asr-table information flow-control—Show flow control information fogrp-table—Show fogrp-table information global-table—Show global-table information hw-status—Show hw-status interface-vlan—Show interface-vlan information mac—Show mac information mcast—Show mcast information pif—Show interface information route—Show route information semaphore—Show semaphore information stats—Show fp statistics status—Show status syn-cookie—Show syn-cookie vft—Show vft table information vlan—Show vlan information.
all	Displays all NP information.

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
3.1	This is command was introduced.

Usage Guidelines

The **show np** command displays the amount of time thresholds were reached in each NP.

Examples

The following is sample output from the **show np** command in single mode:

```
hostname# show np
          MAX    FREE  THRESH_0  THRESH_1  THRESH_2
NP1 (ingress) 32768 32768          0          0          0
    (egress) 521206 521206          0          0          0
NP2 (ingress) 32768 32768          0          0          0
    (egress) 521206 521206          0          0          0
NP3 (ingress) 32768 32768          0          0          0
    (egress) 521206 521206          0          0          0
hostname(config-ctx)#
```

The following is sample output from the **show np asr-table** command in single mode:

```
hostname# show np 1 asr-table all
-----
                        ASR Table (NP-1)
-----
ASR Group |   Vlan Entries in ASR Group (0 denotes empty slot)
-----
          1 |         0         0         0         0         0         0         0         0
...
          32 |         0         0         0         0         0         0         0         0
-----
hostname#
```

The following is sample output from the **show np 1 flow-control** command in single mode:

```
hostname# show np 1 flow-control
Flow control for np 1
REGISTER      ADDRESS      DATA
i_tx_prob     0x30000000  0x7f7f7f7f
i_rand_num    0x30000100  0x33994fbb
i_fq_th       0xa0400020  0x00000000
e_tx_prob     0xb0000000  0x7f7f7f7f
e_rand_num    0xb0001000  0x7f7f7f7f
p0_twin_th    0xa0400100  0x0007ffff
p1_twin_th    0xa0400200  0x0007ffff
e_p0_ewma_th  0xa0400400  0x0007ffff
e_p1_ewma_th  0xa0400800  0x0007ffff
ewma_k        0xa0400040  0x00000000
ewma_t        0xa0400080  0x00000000
```

```
res_data_cfg          0xa0000880  0x00000003
```

The following is sample output from the **show np 1 fogrp-table all** command in single mode:

```
hostname# show np 1 fogrp-table all
```

```
-----
                        Failover Group Table (NP-1)
-----
Failover Group ID          : 0
My MAC address             : 0005.9a38.8100
Other MAC address          : 0000.0000.0000
Flags                       : 0x1
  |- Failover Stop Traffic  : 0
  |- Logical Update Enabled : 0
  |- Logical Update Sync HTTP : 0
  |- Logical Update Force Sync : 0
  |- Failover Active        : 1
-----
```

The following is sample output from the **show np 1 global-table** command in single mode:

```
hostname# sh np 1 global-table
```

```
...
-----
                        Global Table (NP-1)
-----
Admin VCID                 : 1
Global Flags                : 0x2000
  |- Virtual Mode           : 0
  |- Failover               : 0
  |- Failover State         : 1
  |- Logical Update         : 0
  |- LU_Sync_HTTP           : 0
  |- Fixup ICMP             : 0
  |- Fixup ICMP Error       : 0
LU Interface                : 0
LU Time                     : 15000
DestMAC Address of LU interface : 0x000000000000
SrcMAC Address of LU interface : 0x000000000000
Vlan ID in LU packet        : 0
Type for LU packets         : 0xaaaa
Originating blade           : 0
-----
```

```
hostname#
```

The following is sample output from the **show np 1 hw-status** command in single mode:

```
hostname# sh np 1 hw-status
```

```
Hw status for np 1
REGISTER      ADDRESS      DATA
my_tb         0xa0004080  0x00000000
local_tb      0xa0004100  0x80000000
local_mc_tb   0xa0004200  0x80000000
init_done     0xa0008200  0xffff8000
ready         0xa0040020  0x80000000
pll_lock      0xa0000220  0x00000000
bcb_fq_th_0   0xa0001010  0x03000000
bcb_fq_th_1   0xa0001020  0x05000000
bcb_fq_th_2   0xa0001040  0x0a000000
bcb_fq_th_GT  0xa0001080  0x40000000
ppc_boot_redir 0x38000117  0x00000000
ppc_watchdog  0xa0004800  0x00000000
thread_enable 0xa0008020  0xffffffff
```



```

gfh_data          0x24c00030  0x00000000
i_max_dispatch    0x24400c40  0x80000000
e_max_dispatch    0x24400c50  0x80000000
semaphore         0x25000180  0x00000000
tp_ds_map         0xa0000140  0aaaaaaaa
e_sdm_stack_th    0xa0001800  0x80000000
fq_es_max         0xa0002100  0x00000000
fq_es_th_0        0xa0002010  0x06000000
fq_es_th_1        0xa0002020  0x08000000
fq_es_th_2        0xa0002040  0x20000000
discard_qcb       0xa0001400  0x00000029
bw_alloc          0xa0002800  0x00000000
fcb_fq_size       0xa0002200  0x40000000
dmu_cfg_A         0xa0010010  0x00000000
dmu_cfg_B         0xa0010020  0x00000000
dmu_cfg_C         0xa0010040  0x00000000
dmu_cfg_D         0xa0010080  0x00000001
qd_ac            0xa0024000  0x00000000
nightly-fx1/admin(config)#

```

The following is sample output from the **show np 1 interface-vlan** command in single mode:

```
hostname# sh np 1 interface-vlan 1
```

WARNING: Vlan is shared by multiple contexts

```
-----
                        Interface Statistics Counters (NP-1)
-----
```

```

Vlan Number          : 1
Total Number of Packets RCV      : 0
Total Number of Packets TX       : 0
Total Number of Bytes RCV       : 0
Total Number of Bytes TX        : 0
Total Number of Packets Dropped  : 0
hostname#

```

The following is sample output from the **show np 1 mac** command in single mode:

```

hostname# sh np 1 mac
Number of mac-address entries = 0
hostname#

```

The following is sample output from the **show np 1 mcast** command in single mode:

```
hostname# sh np 1 mcast
```

```
-----
                        Fast Path Multicast Statistics Counters (NP-1)
-----
```

```

MULTICAST_DROP: Destination IP address not class_D      : 0
MULTICAST_DROP: OSPF not enabled                        : 0
MULTICAST_DROP: RIP not enabled                        : 0
MULTICAST_DROP: Not UDP packet                         : 0
MULTICAST_DROP: Leaf not active                        : 0
MULTICAST_DROP: Leaf marked for deletion               : 0
MULTICAST_DROP: Dest port equal to 0                   : 0
MULTICAST_CNT  : Control packet sent to PC              : 0
MULTICAST_CNT  : Data packet received                  : 0
MULTICAST_CNT  : Data packet sent out                  : 0
MULTICAST_CNT  : Look up miss                          : 0
MULTICAST_CNT  : Look up hit                           : 0
MULTICAST_CNT  : Sent to other NP                      : 0
MULTICAST_CNT  : Sent to NP 3                          : 0

```

show np

```

MULTICAST_CNT : IGMP update received           : 0
MULTICAST_CNT : A200 packets received          : 0
MULTICAST_CNT : Leaf insertion successful       : 0
MULTICAST_CNT : Duplicate_entry                 : 0
hostname#

```

The following is sample output from the **show np 1 route** command in single mode:

```

hostname# sh np 1 route
Number of routes = 0
hostname#

```

The following is sample output from the **show np 1 semaphore** command in single mode:

```

hostname# sh np 1 semaphore
Showing Semaphore Information for np 1

```

ThreadNum	SemNum	SemVal	Valid	Pending
0	0	0x02e09020	N	N
	1	0x00000000	N	N
1	0	0x00000037	N	N
	1	0x00000000	N	N
2	0	0x024381e8	Y	N
	1	0x00000000	N	N
3	0	0x02e0d098	N	N
	1	0x00000000	N	N
4	0	0x00000000	N	N
	1	0x00000000	N	N
5	0	0x00000000	N	N
	1	0x00000000	N	N
6	0	0x00000000	N	N
	1	0x00000000	N	N
7	0	0x00000000	N	N
	1	0x00000000	N	N
8	0	0x00000000	N	N
	1	0x00000000	N	N
9	0	0x00000000	N	N
	1	0x00000000	N	N
10	0	0x00000000	N	N
	1	0x00000000	N	N
11	0	0x00000000	N	N
	1	0x00000000	N	N
12	0	0x00000000	N	N
	1	0x00000000	N	N
13	0	0x00000000	N	N
	1	0x00000000	N	N
14	0	0x00000000	N	N
	1	0x00000000	N	N
15	0	0x0282ae38	N	N
	1	0x00000000	N	N
16	0	0x00000000	N	N
	1	0x00000000	N	N
17	0	0x00000000	N	N
	1	0x00000000	N	N
18	0	0x00000000	N	N
	1	0x00000000	N	N
19	0	0x00000000	N	N
	1	0x00000000	N	N
20	0	0x00000000	N	N
	1	0x00000000	N	N
21	0	0x00000000	N	N
	1	0x00000000	N	N
22	0	0x00000000	N	N
	1	0x00000000	N	N

```

23      0      0x0282ae38      N      N
        1      0x00000000      N      N
24      0      0x00000000      N      N
        1      0x00000000      N      N
25      0      0x00000000      N      N
        1      0x00000000      N      N
26      0      0x00000000      N      N
        1      0x00000000      N      N
27      0      0x0282ae38      N      N
        1      0x00000000      N      N
28      0      0x00000000      N      N
        1      0x00000000      N      N
29      0      0x00000000      N      N
        1      0x00000000      N      N
30      0      0x00000000      N      N
        1      0x00000000      N      N
31      0      0x82812799      N      N
        1      0x00000000      N      N
hostname#

```

The following is sample output from the **show np 1 stats** command in single mode:

```

hostname# sh np 1 stats
-----
Fast Path 64 bit Global Statistics Counters (NP-1)
-----
PKT_MNG: total packets (dot1q) rcvd           : 93605
PKT_MNG: total packets (dot1q) sent           : 0
PKT_MNG: total packets (dot1q) dropped        : 0
PKT_MNG: TCP packets received                 : 0
PKT_MNG: UDP packets received                 : 0
PKT_MNG: ICMP packets received               : 0
PKT_MNG: ARP packets received                 : 80259
PKT_MNG: other protocol pkts received         : 0
PKT_MNG: default (no IP/ARP) dropped          : 0
SESS_MNG: sessions created                    : 0
SESS_MNG: sessions embryonic to active        : 0
SESS_MNG: sessions deleted                    : 0
SESS_MNG: session lookup hits                 : 0
SESS_MNG: session lookup misses              : 0
SESS_MNG: embryonic lookup hits               : 0
SESS_MNG: embryonic lookup misses            : 0
-----
Fast Path 32 bit Global Statistics Counters (NP-1)
-----
SESS_MNG: insert errors                       : 0
SESS_MNG: embryonic to active errors          : 0
SESS_MNG: delete errors                      : 0
PKT_MNG: packets to NP-3                     : 0
PKT_MNG: packets from NP-3                   : 1795
PKT_MNG: packets to FWSM                     : 1794
PKT_MNG: packets from FWSM                   : 0
PKT_MNG: packets sent to other blade         : 0
PKT_MNG: packets rcv from other blade        : 0
PKT_MNG: pkt drop (12 checks)                 : 13346
PKT_MNG: pkt drop (13 checks)                 : 0
PKT_MNG: pkt drop (14 checks)                 : 0
PKT_MNG: pkt drop (rate limiting)            : 0
PKT_MNG: pkt drop (A200)                     : 0
LU_MNG: UDP packets sent by FP ok             : 0
LU_MNG: TCP packets sent by FP ok            : 0
LU_MNG: LU packets sent by SP ok             : 0
LU_MNG: LU packets sent errors               : 0
LU_MNG: UDP packets received for FP ok       : 0

```

```

LU_MNG: TCP packets received for FP ok           : 0
LU_MNG: LU packets received for SP ok             : 0
LU_MNG: LU packets received errors                : 0
LU_MNG: LU packets redirected to NP3              : 0
LU_MNG: LU packets returned by NP3                : 0
TLV_MNG: indications sent                        : 0
TLV_MNG: wrong tlv type (pkt dropped)             : 0
DBG_MNG: delete indications sent                  : 0
DBG_MNG: TLV4 received                           : 0
DBG_MNG: embryonic leaves deleted                 : 0
RTL_MNG: Route Lookup miss (pkt drop)             : 0
RTL_MNG: ARP Lookup miss                         : 0
RTL_MNG: MAC Relearns forced                     : 0
RTL_MNG: MAC Relearns forced aborted              : 0
AGE_MNG: Aging threads launched                   : 2099132
AGE_MNG: Aging threads aborted                    : 0
AGE_MNG: Aging ropes completed                    : 524783
AGE_MNG: Aging Errors (no flag set)               : 0
AGE_MNG: Aging Errors (no timeout set)            : 0
PKT_MNG: PKT_DROP_DHCP_INGR                      : 0
PKT_MNG: PKT_DROP_MULTIC_BROADC_INGR             : 0
PKT_MNG: PKT_DROP_A200_INGR                      : 0
PKT_MNG: PKT_DROP_ARP_INGR                      : 80259
PKT_MNG: PKT_DROP_A300_INGR                      : 0
PKT_MNG: PKT_DROP_NOT_DOT1Q_INGR                 : 2130195
PKT_MNG: PKT_DROP_A200_EGR                      : 0
PKT_MNG: PKT_DROP_A200_EMBR_LEAF_NON_ACTIVE      : 0
PKT_MNG: PKT_DROP_A200_EMBR_LEAF_MARK_DEL        : 0
PKT_MNG: PKT_DROP_A200_NAT_LEAF_NON_ACTIVE       : 0
PKT_MNG: PKT_DROP_A200_NAT_LEAF_MARK_DEL         : 0
PKT_MNG: PKT_DROP_A200_TLV_UPDATE_LEAF_NON_ACTIVE : 0
PKT_MNG: PKT_DROP_A200_TLV_UPDATE_LEAF_MARK_DEL  : 0
PKT_MNG: PKT_DROP_A200_TLV_DEL_LEAF_NON_ACTIVE   : 0
PKT_MNG: PKT_DROP_A200_TLV_DEL_LEAF_MARK_DE     : 0
PKT_MNG: PKT_DROP_A200_LINK_DATA_CH_FAIL        : 0
PKT_MNG: PKT_DROP_A200_LEAF_INSERTION_FAIL      : 0
PKT_MNG: PKT_DROP_L4_FIXUP_ACK                   : 0
PKT_MNG: PKT_DROP_L4_FIXUP_SYN                   : 0
PKT_MNG: PKT_DROP_L4_FIXUP_RST                   : 0
PKT_MNG: PKT_DROP_L4_FIXUP_SYN_ACK               : 0
RL_MNG: session miss packet dropped               : 0
RL_MNG: other protocol or ICMP dropped            : 0
RL_MNG: packet to PIX dropped                     : 0
RL_MNG: packet to Fixup-PC dropped                : 0
RL_MNG: packet to Fixup-SP dropped                : 0
PF_MNG: pause frames sent (x3)                   : 0
PKT_MNG: PKT_DROP_INVALID_GROUP_ID               : 0
PKT_MNG: PKT_DROP_INVALID_PAIR_VLAN              : 0
PKT_MNG: PKT_DROP_L4_BAD_FLAGS                   : 0
PKT_MNG: PKT_DROP_L4_SEND_RST_A300               : 0
PKT_MNG: PKT_DROP_L4_SEND_RST_ALREADY_RST        : 0
PKT_MNG: PKT_DROP_L4_SYN_ACK_SAME_DIRECT_OF_SYN  : 0
PKT_MNG: PKT_DROP_L4_ACK_NOT_ACK_THE_SYN_ACK_INS : 0
PKT_MNG: PKT_DROP_L4_ACK_NOT_ACK_THE_SYN_ACK_OUT : 0
PKT_MNG: PKT_DROP_L4_ACK_RCV_IN_WRONG_DIRECTION : 0
PKT_MNG: PKT_DROP_L4_BAD_CHECKSUM                : 0
PKT_MNG: PKT_DROP_PIF_LOOKUP_FAIL                : 0
PKT_MNG: PKT_DROP_BACK_TO_BACK_PACKET            : 0
CNT_NUMBER_FULL_OPEN_INDICATION_TO_BE_SENT       : 0
CNT_NUMBER_FULL_OPEN_INDICATION_SENT             : 0
IPv6 packet received                             : 0
IPv6 packet sent                                 : 0
IPv6 packet received from PC                     : 0
IPv6 packet sent to PC                           : 0

```

```
hostname#
```

The following is sample output from the **show np 1 status** command in single mode:

```
hostname# sh np 1 status
Showing the np 1 status
      NP      VALUE      STATUS
      1      0x00000005      Unknown Code
hostname#
```

The following is sample output from the **show np 1 syn-cookie** command in single mode:

```
hostname# sh np 1 syn-cookie
-----
                        Fast Path Syn Cookie Statistics Counters (NP-1)
-----
SYN_COOKIE: Syn cookie secret wheel index                : 94
SYN_COOKIE: Total number of SYNs intercepted              : 0
SYN_COOKIE: Total number of ACKs intercepted              : 0
SYN_COOKIE: Total number of ACKs dropped after lookup     : 0
SYN_COOKIE: Total number of ACKs successfully validated   : 0
SYN_COOKIE: Total number of ACKs Dropped: Secret Expired : 0
SYN_COOKIE: Total number of ACKs Dropped: Invalid Sequence : 0
SYN_COOKIE: Total number of Syn Cookie Entries inserted by NP3 : 0
SYN_COOKIE: ACKs dropped: Syn cookie ses not yet established : 0
SYN_COOKIE: Leaf allocation failed                        : 0
SYN_COOKIE: Leaf insertion failed                        : 0
hostname#
```

Related Commands

Command	Description
show np block	Displays NP block information.
show np pc	Displays NP program counters.
show np acl-notification	Displays the status of NP access list notifications.

show np acl-notification

To display the status of NP access list notifications, use the **show np acl-notification** command in privileged EXEC mode.

show np acl-notification

Syntax Description

acl-notification Displays the status of NP access list notifications.

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
3.1	This command was introduced.

Examples

The following is sample output from the **show np acl-notification** command in single mode:

```
hostname# show np acl-notification
acl-notification on
hostname(config-ctx)#
```

Related Commands

Command	Description
show np	Displays extended NP information.
show np block	Displays NP block information.
show np pc	Displays the status of NP program counters.

show np block

To display the buffer information in all the network processors, use the **show np block** command in privileged EXEC mode.

show np block

Syntax Description	block	Shows the maximum and free blocks in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.

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
	3.1	This is command was introduced.

Usage Guidelines	The show np block command displays the amount of time thresholds were reached in each NP.

Examples	The following is sample output from the show np block command in single mode:

```
hostname# show np block
          MAX    FREE    THRESH_0    THRESH_1    THRESH_2
NP1 (ingress) 32768 32768           0           0           0
      (egress) 521206 521206           0           0           0
NP2 (ingress) 32768 32768           0           0           0
      (egress) 521206 521206           0           0           0
NP3 (ingress) 32768 32768           0           0           0
      (egress) 521206 521206           0           0           0
hostname(config-ctx) #
```

Table 27-5 show np block Fields

Field	Description
NP1	The network processor number.
MAX	The maximum number of blocks the NP can use.

Table 27-5 *show np block Fields (continued)*

Field	Description
FREE	The number of free blocks remaining before the NP reaches its threshold.
THRESH_0	The thresholds are the limits a network processor can handle before it takes an action such as sending a pause frame, dropping new packets, or dropping the currently assembled packet. Threshold 0 is set as 48 buffers, Threshold 1 is set as 80 buffers, and Threshold 2 is set as 160 buffers.

Related Commands

Command	Description
show np	Displays extended NP information.
show np pc	Displays NP program counters.
show np acl-notification	Displays the status of NP access list notifications.

show np pc

To display the program counter in each of the 32 threads in all the network processors, use the **show np pc** command in privileged EXEC mode.

show np pc

Syntax Description	pc	Shows the maximum and free pcs in each side (ingress or egress) in each NP and the amount of time thresholds were reached in each NP.

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
	3.1	This is command was introduced.

Examples	The following is sample output from the show np pc command in single mode:

```
hostname# show np pc
THREAD:PC (NP1/NP2/NP3)
 0:0000/0000/0000  1:0000/0000/0000  2:5c4a/45ff/0000  3:0000/0000/0000
 4:0000/0000/0000  5:0000/0000/0000  6:0000/0000/0000  7:0000/0000/0000
 8:0000/0000/0000  9:0000/0000/0000 10:0000/0000/0000 11:0000/0000/0000
12:0000/0000/0000 13:0000/0000/0000 14:0000/0000/0000 15:0000/0000/0000
16:0000/0000/0000 17:0000/0000/0000 18:0000/0000/0000 19:0000/0000/0000
20:0000/0000/0000 21:0000/0000/0000 22:0000/0000/0000 23:4628/0000/0000
24:0000/0000/0000 25:0000/0000/0000 26:0000/0000/0000 27:0000/0000/0000
28:0000/0000/0000 29:0000/0000/0000 30:0000/0000/0000 31:0000/0000/0000
hostname(config-ctx)#
```

Table 27-6 show np pc Fields

Field	Description
THREAD	Displays the program counter in each of the 32 threads in all the network processors

 show np pc

Related Commands	Command	Description
	show np	Displays extended NP information.
	show np block	Displays NP block information.
	show np acl-notification	Activates NP access list notifications.

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	<i>area_id</i>	(Optional) ID of the area that is associated with the OSPF address range.
	<i>pid</i>	(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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show ip ospf).
	3.1(1)	This command was changed from show ip ospf to show ospf .

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:

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

Release	Modification
1.1(1)	This command was introduced (as show ip ospf border-routers).
3.1(1)	This command was changed from show ip ospf border-routers to show ospf border-routers .

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
```

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 FWSM, 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-originate | adv-router addr]
```

```
show ospf [pid [area_id]] database database-summary
```

Syntax Description

<i>addr</i>	(Optional) Router address.
adv-router	(Optional) Advertised router.
<i>area_id</i>	(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.
<i>lsid</i>	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
<i>pid</i>	(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		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced (as show ip ospf database).
3.1(1)	This command was changed from show ip ospf database to show ospf database .

Usage Guidelines

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	<i>interface_name</i>	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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show ip ospf flood-list).
	3.1(1)	This command was changed from show ip ospf flood-list to show ospf flood-list .

Usage Guidelines 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

show ospf flood-list

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	<i>interface_name</i>	(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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show ip ospf interface).
	3.1(1)	This command was changed from show ip ospf interface to show ospf interface .

Usage Guidelines	When used without the <i>interface_name</i> 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)
```

■ show ospf interface

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.
	<i>interface_name</i>	(Optional) Name of the interface for which to display neighbor information.
	<i>nbr_router_id</i>	(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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show ip ospf neighbor).
	3.1(1)	This command was changed from show ip ospf neighbor to show ospf neighbor .

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

 show ospf neighbor

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

<i>interface_name</i>	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.
<i>nbr_router_id</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show ip ospf request-list).
3.1(1)	This command was changed from show ip ospf request-list to show ospf request-list .

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

<i>interface_name</i>	Name of the interface for which to display neighbor information.
<i>nbr_router_id</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show ip ospf retransmission-list).
3.1(1)	This command was changed from show ip ospf retransmission-list to show ospf retransmission-list .

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. 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:

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

Release	Modification
1.1(1)	This command was introduced (as show ip ospf summary-address).
3.1(1)	This command was changed from show ip ospf summary-address to show ospf summary-address .

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
```

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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show ip ospf virtual-links).
	3.1(1)	This command was changed from show ip ospf virtual-links to show ospf virtual-links .

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 Vlan101, 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 pc conn

To display information about connections, address translation, and local host information that are maintained on the control-point, use the **show pc conn** command in privileged EXEC mode. This command also shows the number of TCP, UDP, and embryonic connections, as well as those connections most used.

show pc conn [count] | local-host | xlate

Syntax Description

count	Shows a count of the current active connections maintained on the control-point, along with a high water mark of most connections used on the control-point.
local-host	Shows the total number of active TCP, UDP, and embryonic connections maintained on the control-point.
xlate	Shows the total number of active address translations maintained on the control-point.

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
2.3(1)	This command was introduced.

Usage Guidelines

All the connections that are being processed by the control-point on the FWSM display. These connections are being processed in software on the central CPU, not in hardware.

Examples

The following example shows how to display connection information:

```
hostname# show pc conn
```

```
2 in use, 10230 most used
UDP out 14.1.26.199:53 in 10.10.10.119:53 idle 0:00:00 flags
UDP out 14.1.26.199:53 in 10.10.10.119:53 idle 0:00:00 flags
```

Related Commands

Command	Description
show xlate	Shows translations.
show conn	Shows connection information.
show local-host	Shows IP addresses of local hosts.
set connection	Sets connection limits.

show perfmon

To capture information about the performance of the FWSM, use the **show perfmon** command in privileged EXEC configuration mode. To view the output, use the **show console-output** command.

show perfmon [detail]

Syntax Description	detail Displays connection rates that you configure for a specified interval.

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
	1.1(1)	This command was introduced.
	3.2(1)	Added the detail keyword.

Usage Guidelines

The FWSM does not include a serial console port, but some messages are only displayed on a console port, including output from the **show perfmon** and **perfmon** commands. Use the **show output-console** command to view the console buffer, including the **show perfmon** command output.

The **perfmon** command allows you to monitor the FWSM performance. The **show perfmon** command allows you to display the information immediately. The **show perfmon detail** command allows you to display the connection and xlate setup rates in a new output section.

Examples

This example shows how to display information about the FWSM performance:

```
hostname# show perfmon
hostname# show console-output
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

```

This example shows how to display the connection and xlate setup rates.

```

hostname# show perfmon detail
hostname# show console-output
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
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
Xlates for 1 minute = 0/s; 5 minutes = 0/s

```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information.
show console-output	Shows the console buffer.

show pim df

To display the bidirectional DF “winner” for a rendezvous point (RP) or interface, use the **show pim df** command in privileged EXEC mode.

show pim df [**winner**] [*rp_address* | *if_name*]

Syntax Description

<i>if_name</i>	The physical or logical interface name.
<i>rp_address</i>	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.
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:

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

Command History

Release	Modification
3.1(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 privileged EXEC mode.

show pim group-map [**info-source**] [*group*]

Syntax Description

<i>group</i>	(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the FWSM from different clients.

The PIM implementation on the FWSM 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
```

show pim group-map

```
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 FWSM.
	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 privileged EXEC mode.

show pim interface [*if_name* | **state-off** | **state-on**]

Syntax Description	<i>if_name</i>	(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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines The PIM implementation on the FWSM considers the FWSM 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
	mcast-routing	Enables multicast routing on the FWSM.

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in 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:

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

Command History

Release	Modification
3.1(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		
Vlan38	0 /	0 /	0	0 /	0 /	0
Vlan37	0 /	0 /	0	0 /	0 /	0
Vlan36	0 /	0 /	0	0 /	0 /	0
Vlan35	0 /	0 /	0	0 /	0 /	0
Vlan	0 /	0 /	0	0 /	0 /	0
Vlan34	0 /	0 /	0	0 /	0 /	0
Vlan22	0 /	0 /	0	0 /	0 /	0
Vlan20	0 /	0 /	0	0 /	0 /	0
Vlan	0 /	0 /	0	0 /	0 /	0
Vlan124	0 /	0 /	0	0 /	0 /	0
Vlan136	0 /	0 /	0	0 /	0 /	0
Vlan137	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 privileged EXEC mode.

```
show pim neighbor [count | detail] [interface]
```

Syntax Description

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.
interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

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
3.1(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 FWSM considers the FWSM itself to be a PIM neighbor. Therefore, the FWSM interface is shown in the output of this command. The IP address of the FWSM 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 FWSM.

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in 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:

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

Release	Modification
3.1(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 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:

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

Command History

Release	Modification
3.1(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 mrrib 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 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:

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

Release	Modification
3.1(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 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:

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

Command History	Release	Modification
	3.1(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 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:

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

Command History	Release	Modification
	3.1(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

Valid PIM Packets          Received      Sent
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
```

■ show pim traffic

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 privileged EXEC mode.

show pim tunnel [*if_name*]

Syntax Description

<i>if_name</i>	(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:

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

Command History

Release	Modification
3.1(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 processes

To display a list of the processes that are running on the FWSM, use the **show processes** command in privileged EXEC mode.

show processes [cpu-hog | memory | internals]

Defaults

By default this command displays the processes running on the FWSM.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **show processes** command allows you to display a list of the processes that are running on the FWSM.

The command can also help determine what process is using the CPU, with the optional **cpu-hog** argument. A process is flagged if it is hogging the CPU for more than 100 milliseconds. 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.

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 and is accurate to within one millisecond, 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.

With the scheduler and total summary lines, you can run two consecutive **show process** 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 FWSM:

```
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	FragDBG
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 processes cpu
```

MAXHOG	NUMHOG	LASTHOG	Process
7720	4	110	Dispatch Unit
7870	331	1010	Checkheaps
(other lines deleted for brevity)			
6170	1	6170	CTM message handle

```
hostname(config)# show processes memory
```

Allocs	Allocated (bytes)	Frees	Freed (bytes)	Process
23512	13471545	6	180	*System Main*
0	0	0	0	lu_rx
2	8324	16	19488	vpnlb_thread
(other lines deleted for brevity)				

```
hostname# sho proc 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

■ show processes

```
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 FWSM, 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:

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

Release	Modification
3.1(1)	Support for 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)
```

Command	Description
reload	Reboots and reloads the configuration.

show resource acl-partition

To show the number of memory partitions in multiple context mode, the contexts assigned to each partition, and the number of rules used, use the **show resource acl-partition** command in privileged EXEC mode.

show resource acl-partition [*context*]

Syntax Description

context Shows the partition to which a context is assigned.

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	N/A	N/A	—	—	•

Command History

Release	Modification
2.3(1)	This command was introduced.

Examples

The following is sample output from the **show resource acl-partition** command:

```
hostname# show resource acl-partition
```

```
Total number of configured partitions = 2
```

```
Partition #0
```

```
Mode :exclusive
```

```
List of Contexts :bandn, borders
```

```
Number of contexts :2 (RefCount:2)
```

```
Number of rules :0 (Max:53087)
```

```
Partition #1
```

```
Mode :non-exclusive
```

```
List of Contexts :admin, momandpopA, momandpopB, momandpopC  
momandpopD
```

```
Number of contexts :5 (RefCount:5)
```

```
Number of rules :6 (Max:53087)
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
resource acl-partition	Determines the number of memory partitions for multiple context mode.

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:

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

Command History	Release	Modification
	2.2(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          35.00%
Fixups [rate]     35000          35.00%
Syslogs [rate]    10500          35.00%
Conns             305000         30.50%
Hosts             78842          30.07%
IPsec             7              35.00%
SSH               35             35.00%
Telnet            35             35.00%
Xlates            91749          34.99%
All               unlimited
```

Table 27-7 *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 FWSM 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.

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	20.00%
	silver	1	CA	17000	17000	10.00%
	bronze	0	CA	8500		
	All Contexts:	3			51000	30.00%
Fixups [rate]	default	all	CA	unlimited		
	gold	1	DA	unlimited		
	silver	1	CA	10000	10000	10.00%
	bronze	0	CA	5000		
	All Contexts:	3			10000	10.00%
Syslogs [rate]	default	all	CA	unlimited		
	gold	1	C	6000	6000	20.00%
	silver	1	CA	3000	3000	10.00%
	bronze	0	CA	1500		
	All Contexts:	3			9000	30.00%
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	9.99%
	bronze	0	CA	13107		
	All Contexts:	3			26214	9.99%
IPSec	default	all	C	5		
	gold	1	D	5	5	50.00%
	silver	1	CA	1	1	10.00%
	bronze	0	CA	unlimited		
	All Contexts:	3			11	110.00%
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	10.00%
	bronze	0	CA	11520		
	All Contexts:	3			23040	10.00%
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

```

Table 27-8 shows each field description.

Table 27-8 *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 FWSM 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 FWSM 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 the resource is unlimited, this display is blank.

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 FWSM.

show resource partition

To view the current, startup, and default partition sizes, use the **show resource partition** command in global configuration mode.

show resource partition

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
Global configuration	•	•	—	—	•

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines The **show resource partition** command lets you plan how to resize memory partitions in multiple context mode using the **size** command. For more information about memory partitions, see the **resource acl-partition** command.

Examples The following is sample output from the **show resource partition** command:

```
hostname(config)# show resource partition
```

Partition Number	Default Size	Bootup Partition Size	Current Configured Size
0	19219	19219	19219
1	19219	19219	19219
2	19219	19219	19219
3	19219	19219	19219
4	19219	19219	19219
5	19219	19219	19219
6	19219	19219	19219
7	19219	19219	19219
8	19219	19219	19219
9	19219	19219	19219
10	19219	19219	19219
11	19219	19219	19219

show resource partition

```

backup tree    19219        19219        19219
-----+-----+-----+-----
      Total    249847        249847        249847

```

```

Total Partition size - Configured size = Available to allocate
      249847        -      249847        =              0

```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource rule	Shows the current allocation of rules.
show running-config resource partition	Shows the current memory partition configuration.
size	Changes the size of a memory partition.

show resource rule

To show the total number of rules available, the default values, current rule allocation, and the absolute maximum number of rules you can allocate per feature, use the **show resource rule** command in privileged EXEC mode. There are a fixed number of rules available on the FWSM, so you might want to reallocate rules between features depending on usage. Features that use rules include access lists, inspections, AAA, and more.

show resource rule [**partition** *number*]

Syntax Description

number	(Optional) In multiple context mode, shows the rule allocation for a particular partition number.
partition	(Optional) In multiple context mode, shows the rule allocation per partition. You can override the global rule allocation for a specific partition if you enter the rule command. To view the global settings set by the resource rule command, use the show resource rule command without a partition number.

Defaults

If you do not specify the **partition** keyword, then the global settings 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	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.2(1)	This command was introduced.
4.0(1)	The partition and <i>number</i> arguments were added.

Usage Guidelines

Use the **resource rule** command to reallocate rules between features; in multiple context mode, the resource rule command sets the allocation globally for all partitions. Use the **rule** command to set the allocation for a specific partition. The **show resource rule** command lets you plan your resource allocation. In multiple context mode, this command shows the global setting for each partition. To see the actual rules allocated for a specific partition, use the **show resource rule partition** command. See the **resource acl-partition** command for more information about partitions.

You can also use the **show np 3 acl count** command to view the number of rules currently being used.

Examples

The following is sample output from the **show resource rule** command in single mode:

```
hostname(config)# show resource rule
```

CLS Rule	Default Limit	Configured Limit	Absolute Max
Policy NAT	1843	1843	10000
ACL	74188	74188	74188
Filter	2764	2764	5528
Fixup	4147	4147	10000
Est Ctl	460	460	460
Est Data	460	460	460
AAA	6451	6451	10000
Console	1843	1843	3686
Total	92156	92156	

Partition Limit - Configured Limit = Available to allocate
 92156 - 92156 = 0

The following is sample output from the **show resource rule partition** command in multiple mode:

hostname(config)# **show resource rule partition 0**

CLS Rule	Default Limit	Configured Limit	Absolute Max
Policy NAT	283	283	833
ACL	10633	10633	10633
Filter	425	425	850
Fixup	1417	1417	2834
Est Ctl	70	70	70
Est Data	70	70	70
AAA	992	992	1984
Console	283	283	566
Total	14173	14173	

Partition Limit - Configured Limit = Available to allocate
 14173 - 14173 = 0

Field descriptions for the **show resource rule** command are shown below:

Field	Description
CLS Rule	Shows the feature types that use rules.
Default Limit	Shows the default limit for each feature.
Configured Limit	Shows the limit you configured using the resource rule command.
Absolute Max	Shows the maximum limit you can assign to a feature using the resource rule command.
Policy NAT	Shows the default, configured, and maximum limits for policy NAT rules.
ACL	Shows the default, configured, and maximum limits for ACEs.
Filter	Shows the default, configured, and maximum limits for filter rules.
Fixup	Shows the default, configured, and maximum limits for inspect rules.

Field	Description
Est Ctl	Shows the default, configured, and maximum limits for established command control rules.  Note The established command creates two types of rules, control and data. Both of these types are shown in the display, but you allocate both rules by setting the number of established commands; you do not set each rule separately. Be sure to double the est value in the resource rule command when comparing the total number of configured rules with the total number of rules shown in the show resource rule command.
Est Data	Shows the default, configured, and maximum limits for established command data rules.  Note The established command creates two types of rules, control and data. Both of these types are shown in the display, but you allocate both rules by setting the number of established commands; you do not set each rule separately. Be sure to double the est value in the resource rule command when comparing the total number of configured rules with the total number of rules shown in the show resource rule command.
AAA	Shows the default, configured, and maximum limits for AAA rules.
Console	Shows the default, configured, and maximum limits for HTTP, Telnet, SSH, and ICMP rules.
Total	Shows the total number of rules for the system under the Default Limit column, and the total number of rules configured under the Configured Limit column.
Partition Limit - Configured Limit = Available to allocate	Shows the system limit (for multiple context mode, this is the partition limit) minus the number of rules you have configured so you can see the number of rules you can still allocate.

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
context	Configures a security context.
resource acl-partition	Sets the number of memory partitions for rules.
resource rule	Reallocates rules between features.
rule	Reallocates rules between features per partition.
show np 3 acl count	Shows the number of rules in use.
show resource acl-partition	Shows the contexts assigned to each memory partition and the number of rules used.

show resource types

To view the resource types for which the FWSM can limit usage per context, 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples The following is sample output from the **show resource types** command:

```
hostname# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Fixups           Fixups/sec
  Syslogs          Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  IPSec           IPSec Mgmt Tunnels
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  MAC Addresses   MAC addresses
  All             All Resources
```

Related Commands

Command	Description
class	Creates a resource class.
context	Adds a security context.

Command	Description
limit-resource	Sets the resource limit for a class.
show resource allocation	Shows the resource allocation for each resource across all classes and class members.
show resource usage	Shows the resource usage of the FWSM.

show resource usage

To view the resource usage of the FWSM 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]
                    [resource {resource_name | all} | detail] [counter counter_name [count_threshold]]
```

Syntax Description

context <i>context_name</i>	(Multiple mode only) Specifies the context name for which you want to view statistics. Specify all for all contexts; the FWSM lists the context usage for each context.
<i>count_threshold</i>	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 <i>count_threshold</i> applies to the current usage. Note To show all resources, set the <i>count_threshold</i> to 0.
counter <i>counter_name</i>	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 allocation. • 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 <i>resource_name</i>	Shows the usage of a specific resource. Specify all (the default) for all resources. 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. • hosts—Hosts that can connect through the FWSM. • ipsec—IPSec sessions. • mac-addresses—For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • ssh—SSH sessions. • 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 <i>n</i>	(Multiple mode only) Shows the contexts that are the top <i>n</i> 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

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
Fixups [rate]	270	535	100000 (S)	0	Summary

U = Some contexts are unlimited and are not included in the total.

S = All contexts are unlimited; 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	1191228	1220084	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	26	27	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	0	0	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
chunk:est-sip	0	0	unlimited	0	admin
chunk:event-mgmt-m	0	0	unlimited	0	admin
chunk:event-mgmt-q	0	0	unlimited	0	admin
...					
Telnet	0	0	5	0	admin
SSH	0	0	5	0	admin
ASDM	0	0	5	0	admin
IPSec	0	0	5	0	admin
Syslogs [rate]	0	0	unlimited	0	admin
aaa rate	0	0	unlimited	0	admin
url filter rate	0	0	unlimited	0	admin
Conns	0	0	20000	0	admin
Xlates	0	0	unlimited	0	admin
tcp conns	0	0	unlimited	0	admin
Hosts	0	0	unlimited	0	admin
udp conns	0	0	unlimited	0	admin
smtp-fixups	0	0	unlimited	0	admin
Conns [rate]	0	0	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-intercept-rate	0	0	unlimited	0	admin
globals	0	0	unlimited	0	admin
np-statics	2	2	unlimited	0	admin
statics	1	1	unlimited	0	admin
nats	1	1	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   1          1          N/A          0 admin
policy-nat-rules     0          0          N/A          0 admin
fixup-rules          32         32          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
Mac-addresses        0          0      65535      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 route

To display a default or static route for an interface, use the **show route** command in privileged EXEC mode.

show route [*interface_name ip_address netmask gateway_ip*]

Syntax Description

<i>gateway_ip</i>	(Optional) IP address of the gateway router (the next-hop address for this route).
<i>interface_name</i>	(Optional) Internal or external network interface name.
<i>ip_address</i>	(Optional) Internal or external network IP address.
<i>netmask</i>	(Optional) Network mask to apply to <i>ip_address</i> .

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
1.1(1)	This command was introduced.

Examples

The following is sample output from the **show route** command:

```
hostname(config)# show route
C   10.30.10.0 255.255.255.0 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
```

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 running-config route	Displays configured routes.

show route-inject

To display all the routes and NAT pools that have been injected, use the **show route-inject** command in privileged EXEC mode.

show route-inject

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
	4.0(1)	This command was introduced.

Usage Guidelines Use the **show route-inject** command in privileged EXEC mode to display the routes and NAT pools that have been injected.

Examples The following is sample output from the **show route-inject** command:

```
hostname(config)# show route-inject
Routes injected:
Address Mask Nexthop Proto Weight Vlan
-----
20.11.111.11
20.11.111.11 255.255.255.0
NATs injected:
Address Mask Nexthop Weight Vlan
-----
20.11.111.11 255.255.255.0
```

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
debug route-inject	Enables debugging of the route-injections that have been configured on FWSM.
route-inject	Injects the connected and static routes and NAT pools configured on FWSM into the MSFC routing table.
show running-config route-inject	Displays the route-injection running configuration.



CHAPTER

28

show running-config through show running-config isakmp Commands

show running-config

To display the configuration that is running on the FWSM, 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.
<i>command</i>	Displays the configuration associated with a specific command.

Defaults

If no arguments or keywords are specified, the entire non-default FWSM configuration displays.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

The **show running-config** command displays the current running configuration on the FWSM.

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.



Note

The device manager commands appear in the configuration after you use it to connect to or configure the FWSM.

Examples

This example show how to display the configuration that is running on the FWSM:

```
hostname# show running-config
: Saved
:
FWSM Version 3.1(0)
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 FWSM
domain-name example.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
```

■ show running-config

```

ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map fwsm_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 ctigbe
    inspect cuseeme
    inspect icmp
  !
terminal width 80
service-policy fwsm_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end

```

Related Commands

Command	Description
configure	Configures the FWSM 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:

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

Command History

Release	Modification
1.1(1)	The show aaa command was introduced.
2.2(1)	The show aaa command was modified to support a LOCAL method.
3.1(1)	This command was changed from show aaa .

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
```

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.
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*)]

Syntax Description

all	(Optional) Shows defaults values, which are otherwise omitted from command output.
(<i>interface-name</i>)	(Optional) The network interface where the AAA server resides.
<i>server-tag</i>	(Optional) The symbolic name of the server group.

Defaults

Omitting the **all** 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:

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

Command History

Release	Modification
1.1(1)	The show aaa-server command was introduced.
3.1(1)	This command was changed from show aaa-server .

Usage Guidelines

Use this command to display the settings for a particular server group. Use the **all** keyword to display default values 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
```

Related Commands

Command	Description
show aaa-server	Displays AAA server statistics.
show running-config aaa-server host	Displays AAA server settings for a specific AAA server.
clear configure aaa-server	Clears the AAA server configuration.

show running-config aaa-server host

To display AAA server statistics for a particular AAA server, use the **show running-config aaa-server host** command in global configuration or privileged EXEC mode.

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *aaa-server-name*

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
host <i>aaa-server-name</i>	Specifies the AAA server by hostname or IP address.
(<i>interface-name</i>)	(Optional) The network interface where the AAA server resides.
<i>server-tag</i>	The symbolic name of the server group.

Defaults

Omitting the **all** 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use this command to display the statistics for a particular server group. Use the **all** keyword to display default values 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 all aaa-server svrgrp1
```

Related Commands

Command	Description
show running-config aaa-server	Displays AAA server settings.
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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show access-group .

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 FWSM, 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 | optimization]

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.
<i>id</i>	Identifies the access list that is displayed.
optimization	Shows optimized access lists.
<i>saddr_ip</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.
4.0(1)	Keyword optimization added.

Usage Guidelines

The **show running-config access-list** command lets you display the current running access list configuration on the FWSM.

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.
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 alias configuration, use the **show running-config alias** command in privileged EXEC mode.

show running-config [**all**] **alias** [*interface_name*]

Syntax Description

all (Optional) Shows all commands, including the commands you have not changed from the default.

interface_name (Optional) Shows the **alias** commands for the specified interface.

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
Global configuration	•	—	—	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show alias .

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 [all] arp

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	3.1(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 [all] arp timeout

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(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 FWSM 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 [all] arp-inspection

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show running-config pdm).
3.1(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 FWSMs 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 history enable
hostname#
```

Related Commands

Command	Description
clear configure asdm	Removes all asdm commands from the running configuration.

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:

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

Command History

Release	Modification
1.1(1)	The show auth-prompt command was introduced.
3.1(1)	This command was changed from show auth-prompt .

Usage Guidelines

After you set the authentication prompt, use the **show running-config auth-prompt** command to view the current prompt text.

Examples

This example shows the use of the **show running-config auth-prompt** command to show the authentication prompt configuration:

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please sign in.
auth-prompt accept Welcome. Unauthorized access strictly prohibited.
auth-prompt reject Credentials invalid.
hostname(config)#
```

Related Commands

auth-prompt	Set the user authentication prompts.
clear configure auth-prompt	Reset the user authentication prompts to the default value.

show running-config auto-update

To display the **auto-update** commands in the running configuration, use the **show running-config auto-update** command in privileged EXEC mode.

show running-config [all] auto-update

Syntax Description	all	(Optional) Shows all 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples	The following is sample output from the show running-configuration auto-update command:

```
hostname# show running-config auto-update
auto-update poll-period 1 1
auto-update server http://10.1.1.1:1741/
```

Related Commands	Command	Description
	auto-update device-id	Sets the FWSM device ID for use with an Auto Update Server.
	auto-update poll-period	Sets how often the FWSM 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 FWSM 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 class

To display the resource class configuration, use the **show running-config class** command in privileged EXEC mode.

show running-config [**all**] **class** *class_name*

Syntax Description

all	(Optional) Show all running resource class configuration, including default.
<i>class_name</i>	(Optional) Text for the class name; the text can be up to 20 characters in length.

Defaults

By default, all classes 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	System
Privileged EXEC	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

The following is sample output from the **show running-config class** command:

```
hostname# show running-config class gold
limit-resource all 3%
limit-resource rate syslogs 500
```

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.

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 FWSM using Telnet.
motd	(Optional) Displays the message-of-the-day banner.

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
1.1(1)	The show banner command was introduced.
3.1(1)	This command was changed to show running-config banner .

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-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** {**regex** | **inspect** [*protocol*]}]

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
<i>class_map_name</i>	(Optional) Shows the running configuration for a class map name.
inspect	(Optional) Shows inspection class maps.
<i>protocol</i>	(Optional) Specifies the type of application map you want to show. Available types include: http 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.
4.0(1)	The type keyword was added.

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 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) Shows all 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:

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

Command History	Release	Modification
	3.1(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 FWSM, 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 FWSM, 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 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:

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

Command History	Release	Modification
	1.1(1)	The show console timeout command was introduced.
	3.1(1)	This command was changed to show running-config console timeout .

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 FWSM.
	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.

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	N/A	N/A	—	—	•

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples	The following is sample output from the show running-config context command:

```
hostname# show running-config context

admin-context admin
context admin
  allocate-interface vlan100
  config-url disk:/admin.cfg
!

context A
  allocate-interface vlan200
  config-url disk:/A.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.

Command	Description
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

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:

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

Release	Modification
3.1(1)	This command was introduced.

Command History

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#
```

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.

Related Commands

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM.
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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show crypto dynamic-map .

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, }
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 FWSM.
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:

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

Command History	Release	Modification
	1.1(1)	The show crypto ipsec command was introduced.
	3.1(1)	This command was changed to show running-config crypto ipsec .

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
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 FWSM.
	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:

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

Command History

Release	Modification
1.1(1)	The show crypto isakmp command was introduced.
3.1(1)	This command was changed to show running-config crypto isakmp .

Examples

The following example issued in global configuration mode, displays information about the ISAKMP configuration:

```
hostname(config)# show running-config crypto 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 FWSM.
show 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show crypto map .

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
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.
	isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM.
	show isakmp sa	Displays IKE runtime SA database with additional information.

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:

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

Release	Modification
3.1(1)	This command was introduced.

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:

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

Release	Modification
3.1(1)	This command was introduced.

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 is sample 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:

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

Release	Modification
3.1(1)	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
```

Command	Description
dns domain-lookup	Enables the FWSM 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 FWSM 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 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:

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

Command History	Release	Modification
	1.1(1)	The show domain-name command was introduced.
	3.1(1)	This command was changed to showrunning-config 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 FWSM hostname.

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:

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

Release	Modification
1.1(1)	The show enable command was introduced.
3.1(1)	This command was changed to show running-config enable .

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
```

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 [all] established

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show established .

Examples	This example shows how to display inbound connections that are based on established connections: <pre>hostname# show running-config established</pre>

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:

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

Command History

Release	Modification
3.1(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
hostname#
```

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show filter .

Usage Guidelines

The **show running-config filter** command displays the filtering configuration for the FWSM.

Examples

The following is sample output from the **show running-config filter** command, and shows the filtering configuration for the FWSM:

```
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 FWSM.
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 FWSM.
filter url	Directs traffic to a URL filtering server.

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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	The show fragment command was introduced.
3.1(1)	This command was changed to show running-config fragment .

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **show running-config ftp mode** command displays the client mode that is used by the FWSM when accessing an FTP server.

Examples

The following examples shows 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 FWSM when accessing an FTP server.

show running-config ftp-map

To show the FTP maps that have been configured, use the **show running-config ftp-map** command in privileged EXEC mode.

show running-config ftp-map *map_name*

Syntax Description

map_name Displays configuration for the specified FTP map.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **show running-config ftp-map** command displays the FTP maps that have been configured.

Examples

The following is sample output from the **show running-config ftp-map** command:

```
hostname# show running-config ftp-map ftp-policy
!
ftp-map ftp-policy
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.
request-command deny	Specifies FTP commands to disallow.

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:

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

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show global .

Examples The following is sample output from the **show running-config global** command:

```
hostname# show running-config global
global (outside1) 10 interface
```

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 usernames that are received when tunnels are being negotiated, use the **show running-config group-delimiter** command in global 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:

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

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines Use this command to display the currently configured group-delimiter.

Examples The following example shows a **show running-config group-delimiter** command and its output:

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

Command	Description
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the usernames 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.

show running-config [all] group-policy [name]

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
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:

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

Command History

Release	Modification
3.1(1)	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 gtp-map

To show the GTP maps that have been configured, use the **show running-config gtp-map** command in privileged EXEC mode.

show running-config gtp-map *map_name*

Syntax Description

map_name Displays configuration for the specified GTP map.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **show running-config gtp-map** command displays the GTP maps that have been configured.

Examples

The following is sample output from the **show running-config gtp-map** command:

```
hostname# show running-config gtp-map gtp-policy
!
gtp-map gtp-policy
 request-queue 300
 message-length min 20 max 300
 drop message 20
 tunnel-limit 10000
!
```

Related Commands

Commands	Description
clear service-policy	Clears global GTP statistics.
inspect gtp	
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.

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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

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 FWSM 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 FWSM.
http server enable	Enables the HTTP server.

show running-config http-map

To show the HTTP maps that have been configured, use the **show running-config http-map** command in privileged EXEC mode.

show running-config http-map *map_name*

Syntax Description.	<i>map_name</i>	Displays configuration for the specified HTTP map.

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
	3.1(1)	This command was introduced.

Usage Guidelines	The show running-config http-map command displays the HTTP maps that have been configured.

Examples	The following is sample output from the show running-config http-map command:

```
hostname# show running-config http-map http-policy
!
http-map http-policy
content-length min 100 max 2000 action reset log
content-type-verification match-req-rsp reset log
max-header-length request bytes 100 action log reset
max-uri-length 100 action reset log
!
```

Related Commands	Commands	Description
	class-map	Defines the traffic class to which to apply security actions.
	debug http-map	Displays detailed information about traffic associated with an HTTP map.
	http-map	Defines an HTTP map for configuring enhanced HTTP inspection.

Commands	Description
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **show running-config icmp** command displays the access rules configured for ICMP traffic.

Examples

The following example shows 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 interface

To show the interface configuration in the running configuration, use the **show running-config interface** command in privileged EXEC mode.

show running-config [**all**] **interface** [*mapped_name* | *interface_name*]

Syntax Description

all	(Optional) Shows all interface commands, including the commands you have not changed from the default.
<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.

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:

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

Command History

Release	Modification
1.1(1)	The show interface command was introduced.
3.1(1)	This command was changed to show running-config interface .

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 Vlan 35 and 37 interfaces have not been configured yet, and show the default configuration.

```
hostname# show running-config interface
!
interface Vlan20
  nameif inside
  security-level 100
  ip address 10.86.194.60 255.255.254.0
!
interface Vlan22
  shutdown
```

show running-config interface

```

nameif test
security-level 0
ip address 10.10.4.200 255.255.0.0
!
interface Vlan35
shutdown
no nameif
security-level 0
no ip address
!
interface Vlan37
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 interface bvi

To view the bridge virtual interface configuration in the running configuration, use the **show running-config interface bvi** command in privileged EXEC mode.

show running-config [all] interface bvi *bridge_group_number*

Syntax Description

all	(Optional) Shows all commands, including the commands you have not changed from the default.
<i>bridge_group_number</i>	Specifies the bridge group number as an integer between 1 and 100.

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
3.1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config interface bvi** command:

```
hostname# show running-config interface bvi 1

interface BVI1
```

Related Commands

Command	Description
bridge-group	Groups two transparent firewall interfaces into a bridge group.
clear configure interface bvi	Clears the bridge virtual interface configuration.
interface	Configures an interface.
interface bvi	Enters the interface configuration mode for a bridge group so you can set the management IP address.
ip address	Sets the management IP address for a bridge group.

show running-config ip address

To show the IP address configuration in the running configuration, use the **show running-config ip address** command in privileged EXEC mode.

show running-config ip address [*mapped_name* | *interface_name*]

Syntax Description

<i>interface_name</i>	(Optional) Identifies the interface name set with the nameif command.
<i>mapped_name</i>	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the allocate-interface command.

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:

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

Command History

Release	Modification
3.1(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 the transparent firewall does not have IP addresses associated with the 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
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet1
 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 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:

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

Command History

Release	Modification
3.1(1)	Support for 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
```

```
hostname(config)#
```

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 (Optional) Shows the configuration for the specified interface.
interface_name

Defaults

This command shows the configuration for all interfaces.

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
1.1(1)	This command was introduced.
3.1(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:

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

Command History	Release	Modification
	3.1(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 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples The following example issued in global configuration mode, displays information about the ISAKMP configuration:

```
hostname(config-if)# 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.
	isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM.
	show isakmp sa	Displays IKE runtime SA database with additional information.



show running-config logging through show running-config xlate-bypass Commands

show running-config logging

To display all currently running logging configuration settings, use the **show running-config logging** command in privileged EXEC mode.

show running-config [all] logging [level | disabled]

Syntax Description

all	(Optional) Displays the logging configuration, including commands 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:

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

Command History

Release	Modification
3.1	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
show logging	Shows the current contentsw of the log buffer and other log configuration settings.

show running-config logging rate-limit

To display messages that were disallowed because the current rate limit was exceeded, use the **show running config logging rate-limit** command.

show running-config 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced on the FWSM.
3.1	The show logging rate-limit command was renamed show running-config logging rate-limit .

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

The following example shows how to display the disallowed messages:

```
fwsM/context_name(config)# show logging rate-limit
```

Related Commands

Command	Description
clear logging rate-limit	Resets the rate limit setting to its default value.

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 [all] mac-address-table

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	3.1(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 [all] mac-learn

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	This command was changed from show mac-learn .

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:

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

Command History

Release	Modification
3.1(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 all MAC address lists:

```
hostname(config)# show running-config mac-list
mac-list adc permit 00a0.ca5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.ca5d.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
```

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.ca5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.ca5d.0282 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:

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

Release	Modification
3.1	This command was introduced.

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
```

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the FWSM.
management-access	Configures an internal interface for management access.

show running-config mgcp-map

To show the MGCP maps that have been configured, use the **show running-config mgcp-map** command in privileged EXEC mode.

show running-config mgcp-map *map_name*

Syntax Description.

map_name Displays configuration for the specified MGCP map.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **show running-config mgcp-map** command displays the MGCP maps that have been configured.

Examples

The following is sample output from the **show running-config mgcp-map** command:

```
hostname# show running-config mgcp-map mgcp-policy
!
mgcp-map mgcp-policy
call-agent 10.10.11.5 101
call-agent 10.10.11.6 101
call-agent 10.10.11.7 102
call-agent 10.10.11.8 102
gateway 10.10.10.115 101
gateway 10.10.10.116 102
gateway 10.10.10.117 102
command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.

Commands	Description
show conn	Displays the connection state for different connection types.
show mgcp	Displays information about MGCP sessions established through the FWSM.
timeout	Sets the maximum idle time duration for different protocols and session types.

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The **monitor-interface** command is disabled on all virtual interfaces by default. You need to use the **all** keyword with this command to view the 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.

```
hostname# show running-config monitor-interface
monitor-interface outside
hostname#
hostname# show running-config all monitor-interface
no monitor-interface inside
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 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

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	•	•	•	•	—

Release	Modification
3.1(1)	This command was introduced.

Examples The following is sample output from the **show running-config mroute** command:

```
hostname# show running-config mroute
mroute 10.1.1.0 255.255.255.0 inside 3
```

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show mtu .

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:

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

Command History	Release	Modification
	3.1(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 FWSM.

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
	1.1(1)	The show name command was introduced.
	3.1(1)	This command was changed to show running-config name .

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 fwsm_inside
name 209.165.201.3 fwsm_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 **show running-config nameif** command in privileged EXEC mode.

show running-config nameif [*mapped_name*]

Syntax Description

mapped_name (Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.

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:

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

Command History

Release	Modification
1.1(1)	The show nameif command was introduced.
3.1(1)	This command was changed to show running-config 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(config-if)# show running-config nameif
!
interface Vlan22
  nameif inside
  security-level 100
!
interface Vlan35
  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:

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

Command History	Release	Modification
	1.1(1)	The show names command was introduced.
	3.1(1)	This command was changed to show running-config names .

Usage Guidelines Use with the **names** command.

Examples The following example shows how to display the IP address-to-name conversion:

```
hostname(config-if)# 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

<i>interface_name</i>	(Optional) Name of the network interface.
<i>nat_id</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.1(1)	This command was changed from show nat .

Usage Guidelines

This command displays the maximum connection value for the UDP protocol. Every time the UDP maximum connection value is not set, the value will be displayed as 0 by default and will not be applied.

Examples

The following 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:

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

Release	Modification
3.1(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
```

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 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 <i>obj_grp_id</i>	(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
1.1(1)	This command was introduced.
3.1(1)	This command was changed from show object-group .

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:

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

Command History

Release	Modification
1.1(1)	The show passwd command was introduced.
3.1(1)	This command was changed to show running-config passwd .

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 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:

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

Release	Modification
3.1(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
```

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.
	<i>policy_map_name</i>	(Optional) Shows the running configuration for a policy map name.
	<i>protocol</i>	(Optional) Specifies the type of inspection policy map you want to show. Available types include:
		• dcerpc • esmtplib • http • sip
	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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.
	4.0(1)	The type inspect keywords were added.

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.
```

■ show running-config policy-map

```
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 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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

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 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 <i>command</i>	(Optional) Displays the privilege level for a specific command.
level <i>level</i>	(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:

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

Command History

Release	Modification
1.1(1)	The show privilege command was introduced.
3.1(1)	This command was changed from show privilege .

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 prompt

To view the customized CLI prompt, use the **show running-config prompt** command in privileged EXEC mode.

show running-config prompt

Syntax Description

This command has no arguments or keywords.

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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following is sample output from the **show running-config prompt** command::

```
hostname# show running-config prompt
prompt hostname context
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
prompt	Creates a customized prompt.

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:

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

Command History	Release	Modification
	4.0(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 resource partition

To view the current memory partition configuration, use the **show running-config resource partition** command in privileged EXEC mode.

show running-config [all] resource partition *[number]*

Syntax Description

all	(Optional) Displays the configuration including commands that you have not changed from the default.
<i>number</i>	(Optional) Specifies the partition number, between 0 and 11 by default. If you changed the number of partitions using the resource acl-partition command, the partition numbering starts with 0. So if you have 10 partitions, the partition numbers are 0 through 9.

Defaults

Shows the configuration for all partitions if you do not specify a number.

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
4.0(1)	This command was introduced.

Examples

The following is sample output from the **show running-config resource partition** command:

```
hostname(config)# show running-config resource partition
resource partition 0
    size 40000
resource partition 1
    size 40000
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.

Command	Description
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource partition	Shows the memory partition sizes.
show resource rule	Shows the current allocation of rules.
size	Changes the size of a memory partition.

show running-config rip

To display the information about the RIP configuration, use the **show running-config rip** command in privileged EXEC mode.

show running-config [**all**] **rip** [*interface_name*]

Syntax Description

all	(Optional) Shows all RIP commands, including the commands you have not changed from the default.
<i>interface_name</i>	(Optional) Displays only the RIP commands 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show rip).
3.1(1)	This command was changed from show rip to show running-config rip .

Examples

This example shows how to display RIP information:

```
hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.
debug rip	Displays debug information for RIP.
rip	Configures RIP on the specified interface.

show running-config route

To display the **route** commands in the running configuration, 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced (as show route).
	3.1(1)	This command was changed from show route to show running-config route .

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-inject

To display the route-injection running configuration, use the **show running-config route-inject** command in privileged EXEC mode.

show running-config route-inject

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	•	—	•	•	—

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines Use the **show running-config route-inject** command in privileged EXEC mode to display the route-injection running configuration.

Examples The following is sample output from the **show running-config route-inject** command:

```
hostname(config)# show running-config route-inject
Routes injected:
Address Mask Nexthop Proto Weight Vlan
-----
hostname(config)# interface vlan20
hostname(config-if)# nameif outside
hostname(config-if)# ip address 20.22.211.21 255.255.255.0 standby 20.22.211.22
hostname(config-if)# exit
hostname(config)# access-list acl1 standard permit 23.10.143.20 255.255.255.252
hostname(config)# global (outside) 10 23.10.143.20-23.10.143.23 netmask 255.255.255.0
hostname(config)# global (outside) 10 23.10.143.40-23.10.143.45 netmask 255.255.255.0
hostname(config)# route-inject
hostname(config-route-inject)# redistribute nat access-list acl1 interface outside
-----
```

Related Commands

Command	Description
clear configure route-inject	Removes the routes/NAT pools that were injected into the MSFC routing tables. Additionally, removes the redistribute and route-inject configuration for the user context if you are in multi-mode or system context if in single routed mode.
debug route-inject	Enables debugging of the route-injections that have been configured on the FWSM.
route-inject	Injects the connected and static routes and NAT pools configured on the FWSM into the MSFC routing table.
show route-inject	Displays the routes and NAT pools that have been injected.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced (as show route-map).
3.1(1)	This command was changed from show route-map to show running-config route-map .

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 commands in the router configuration, use the **show running-config router** command in privileged EXEC mode.

show running-config [*all*] **router** [*ospf* [*process_id*]]

Syntax Description	<i>all</i>	Shows all router commands, including the commands you have not changed from the default.
	ospf	(Optional) Displays only the OSPF commands in the configuration.
	<i>process_id</i>	(Optional) Displays the commands for the selected OSPF process.

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
	1.1(1)	This command was introduced (as show ip router).
	3.1(1)	This command was changed from show router to show running-config router .

Examples The following is sample output from the **show running-config router** 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
```

Related Commands	Command	Description
	clear configure router	Clears all router commands from the running configuration.

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 {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 when traffic is IPSec protected.

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
2.2(1)	The show-same-security-traffic command with the inter-interface keyword was introduced.
2.3(1)	Support for the intra-interface keyword was added.
3.1(1)	This command was changed to show running-config same-security-traffic .

Examples

The following is sample output from the **show running-config same-security-traffic** command:

```
hostname# show running-config same-security-traffic
same-security-traffic permit inter-interface
```

Related Commands

Command	Description
same-security-traffic	Permits communication between interfaces with equal security levels.

show running-config service

To display the **service** configuration, use the **show running-config service** command in privileged EXEC mode.

show running-config [all] service

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show service .

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 running-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
	3.1(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 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 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:

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

Command History

Release	Modification
3.1(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	Enable 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 running-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:

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Examples	The following is an example of the show running-config snmp-server command:

```
hostname# show running-config snmp-server
```

Related Commands	Command	Description
	snmp-server	Configures the SNMP server.
	clear snmp-server	Clears the SNMP server configuration.
	show snmp-server statistics	Displays 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:

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

Command History

Release	Modification
3.1(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 FWSM from the specified client or network.
ssh scopy enable	Enables a secure copy server on the FWSM.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the FWSM to using either SSH Version 1 or SSH Version 2.

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:

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

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.1(1)	This command was changed from show static .

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 The following 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.

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

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
3.1(1)	This command was introduced.

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 FWSM.
	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 [all] sysopt

Syntax	Description
all	(Optional) Shows all 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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show sysopt .

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.

Command	Description
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 telnet

To display the current list of IP addresses that are authorized to use Telnet connections to the FWSM, 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 FWSM.

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 FWSM.

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
3.1(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 FWSM:

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User failed to
log in from 209.165.200.225 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User failed to log in from 209.165. 200.225
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:

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

Command History	Release	Modification
	1.1(1)	The show terminal command was introduced.
	3.1(1)	This command was changed to show running-config terminal .

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:

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

Release	Modification
3.1(1)	Support for this command was introduced.

Command History

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
```

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.

Related Commands

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 [all] timeout [protocol]

Syntax Description	all	(Optional) Shows all commands, including the commands you have not changed from the default.
	<i>protocol</i>	(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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	This command was changed from show timeout .

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 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.
<i>name</i>	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:

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

Command History

Release	Modification
3.1(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.

Command	Description
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:

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

Command History

Release	Modification
1.1(1)	The show url-block command was introduced.
3.1(1)	This command was changed from show url-block .

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:

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

Command History

Release	Modification
1.1(1)	The show url-cache command was introduced.
3.1(1)	This command was changed from show url-cache .

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:

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

Command History

Release	Modification
1.1(1)	The show url-server command was introduced.
3.1(1)	This command was changed from show url-server .

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.
<i>name</i>	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:

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

Command History

Release	Modification
1.1(1)	The show username command was introduced.
3.1(1)	This command was changed from show username .

Examples

The following example shows the use of the **show running-config username** command for a user named anyuser:

```
hostname# show running-config username anyuser
username anyuser password .8Tld6ik58/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 FWSM database.
username attributes	Lets you configure AVPs for specific users.

show running-config virtual

To display the IP address of the FWSM 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:

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

Command History

Release	Modification
1.1(1)	The show virtual command was introduced.
3.1(1)	This command was changed from show virtual .

Usage Guidelines

You must be in privileged EXEC mode to use this command.

Examples

The following example shows the output of the **show running-config virtual** command when a virtual HTTP server has already been configured:

```
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-configuration vpn-sessiondb

To display the current set of configured vpn-sessiondb 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-sessiondb 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:

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

Command History	Release	Modification
	3.1(1)	Support for 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 xlate-bypass

To show the xlate bypass configuration, use the **show running-config xlate-bypass** command in privileged EXEC mode. To disable xlate bypass, use the **no** form of this command.

show running-config [all] xlate-bypass

Syntax Description

all (Optional) Shows all 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:

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

Command History

Release	Modification
3.2(1)	This command was introduced.

Examples

The following is sample output from the show running-config xlate-bypass command:

```
hostname# show running-config xlate-bypass
xlate-bypass
```

Related Commands

Command	Description
nat	Configures NAT.
nat-control	Enables NAT control.
same-security-traffic inter-interface	Allows interfaces on the same security level to communicate.
show xlate	Shows current translation and connection information.
xlate-bypass	Enables xlate bypass.



show service-policy through show xlate Commands

show service-policy

To display the configured service policies, use the **show service-policy** command in global configuration mode.

```
show service-policy [global | interface intf] [inspect application_type [option] | set connection |
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

<i>application_type</i>	Sets the application type for which to show inspect statistics. Supported applications include esmtplib , gtp , http , and sip .
<i>dest_ip</i>	The destination IP address of the traffic flow.
<i>dest_mask</i>	The subnet mask of the traffic flow destination IP address.
eq <i>dest_port</i>	(Optional) If you specify the flow protocol to be TCP or UDP, then you can specify the destination port used in the traffic flow.
eq <i>src_port</i>	(Optional) If you specify the flow protocol to be TCP or UDP, then you can specify the source port used in the traffic flow.
flow	(Optional) Specifies a traffic flow for which you want to see the policies that the FWSM would apply to the flow. The arguments and keywords following the flow keyword specify the flow in ip-5-tuple format.
global	(Optional) Limits output to the global policy, which applies to all interfaces.
host <i>dest_host</i>	The host destination IP address of the traffic flow.
host <i>src_host</i>	The host source IP address of the traffic flow.
<i>icmp_control_message</i>	(Optional) If you specify the flow protocol to be ICMP, this argument specifies an ICMP control message of the traffic flow. For valid values for the <i>icmp_control_message</i> argument, enter the show service-policy flow icmp {host src_host src_ip src_mask} {host dest_host dest_ip dest_mask} ? command.
<i>icmp_number</i>	(Optional) If you specify the flow protocol to be ICMP, this argument specifies the ICMP protocol number of the traffic flow.
inspect	(Optional) Limits the output to policies that include an inspect command.
interface <i>intf</i>	(Optional) Displays policies applied to the interface specified by the <i>intf</i> argument, where <i>intf</i> is the interface name given by the nameif command.
<i>option</i>	(Optional) Depending on the application type you specify with the inspect keyword, you can narrow the kind of statistics shown. For esmtplib and http : table—Shows runtime tables such as classification rules. For gtp : pdp-context—Shows the status of GTP PDP contexts. pdpmcb—Shows the status of the GTP PDP Master Control Block requests—Shows the status of GTP requests. statistics—Shows the statistics of of the GTP inspection policy.
<i>protocol</i>	The protocol used in the traffic flow. For valid values for the <i>protocol</i> argument, enter the show service-policy flow ? command.

set connection	(Optional) Limits output to policies that include the set connection command.
<i>src_ip</i>	The source IP address used in the traffic flow.
<i>src_mask</i>	The source IP 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **flow** keyword lets you determine, for any flow that you can describe, the policies that the FWSM 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 default-inspection-traffic**

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.

**Note**

When you configure the **set connection conn-rate-limit** command, the output of **show service-policy** does not show current connection rate and drop count even if the policy is hit:

```
hostname# show service-policy
```

```
Global policy:
Service-policy: 2
Class-map: 2
Set connection policy: conn-rate-limit 10
current conn rate 0, drop 0
```

This is because of a limitation in the network processor.

Examples

The following is sample output from the **show service-policy global** command:

```
hostname# show service-policy global

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns maximum-length 512, packet 0, drop 0, reset-drop 0
      Inspect: ftp, packet 0, drop 0, reset-drop 0
      Inspect: h323 h225, packet 0, drop 0, reset-drop 0
      Inspect: h323 ras, packet 0, drop 0, reset-drop 0
      Inspect: netbios, packet 0, drop 0, reset-drop 0
      Inspect: rsh, packet 0, drop 0, reset-drop 0
      Inspect: skinny, packet 0, drop 0, reset-drop 0
      Inspect: sqlnet, packet 0, drop 0, reset-drop 0
      Inspect: sunrpc, packet 0, drop 0, reset-drop 0
      Inspect: tftp, packet 0, drop 0, reset-drop 0
      Inspect: sip, packet 0, drop 0, reset-drop 0
      Inspect: xdmcp, packet 0, drop 0, reset-drop 0
```

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: global_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: set connection conn-max 10
```

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
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy service-policy	Clears all service policy configurations.
show running-config service-policy	Configures the 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.
<i>ap_name</i>	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.
<i>IMSI_value</i>	Hexadecimal value that identifies the specific IMSI for which statistics are displayed.
interface	(Optional) Identifies a specific interface.
<i>int</i>	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.
<i>IP_address</i>	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.
<i>tunnel_ID</i>	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.
<i>version_num</i>	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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(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_pdpmb | 0 | total_deleted_pdpmb | 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
```

show service-policy inspect gtp

```
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 shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | *statistics*]

Syntax Description	<i>src_ip</i>	(Optional) Displays the information for that address.
	<i>statistics</i>	(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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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:

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

Release	Modification
3.1(1)	This command was introduced.

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 FWSM. 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 FWSM (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 [audio | video]

Syntax Description

audio	Limits output to audio-related information.
video	Limits output to video-related information.

Defaults

If you do not use the audio or video keywords, output contains information for both audio and video, as applicable.

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
3.1(1)	This command was introduced.

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 FWSM. The first session is an audio session 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 a video session 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
  AUDIO 10.0.0.11/22948      172.18.1.22/20798
2      10.0.0.22/52232      172.18.1.33/2000      1
  VIDEO 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
```

If you use the video keyword, output is limited to information about video sessions, as shown in the following example:

```
hostname# show skinny video
LOCAL                                FOREIGN                                STATE
-----
1      10.0.0.22/52232                172.18.1.33/2000                        1
  VIDEO 10.0.0.22/20798                172.18.1.11/22948
```

If you use the audio keyword, output is limited to information about audio sessions, as shown in the following example:

```
hostname# show skinny audio
LOCAL                                FOREIGN                                STATE
-----
1      10.0.0.11/52238                172.18.1.33/2000                        1
  AUDIO 10.0.0.11/22948                172.18.1.22/20798
```

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 snmp-server statistics

To display information about the 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 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
Privileged EXEC	•	•	•	•	

Release	Modification
3.1(1)	Support for 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 Simple Network Management Protocol (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 FWSM, use the **show ssh sessions** command in privileged EXEC mode.

show ssh sessions [*ip_address*]

Syntax Description	<i>ip_address</i> (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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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 FWSM. The Username column lists the login username that has been authenticated for the session.

Examples	The following example shows sample output from 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 FWSM 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System ¹
Privileged EXEC	•	•	•	•	•

1. The **errors** keyword is only available in single mode and the system execution space.

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(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 7.0(0)28
!
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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

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 RPC services from the FWSM.
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 Sun RPC services configuration.

show tcpstat

To display the status of the FWSM TCP stack and the TCP connections that are terminated on the FWSM (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:

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

Release	Modification
1.1(1)	This command was introduced.

Command History

Usage Guidelines The **show tcpstat** command lets you to display the status of the TCP stack and TCP connections that are terminated on the FWSM. The TCP statistics displayed are described in [Table 28](#).

Table 30-2 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 30-2 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

The following is sample output from the **show tcpstat** command:

```
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:

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

Command History

Release	Modification
3.1(1)	The detail and file keywords were added.

Usage Guidelines

The **show tech-support** 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 @ 0xffffd8000, 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 runs, 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 runs, 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	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 Collec
Hwe	0020e301	00d5957c	0053e5c8	0	00d55614	16048/16384	isakmp_time_keep
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 FWSM 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 FWSM
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the FWSM.
show xlate	Displays information about the translation slot.

show traffic

To display interface transmit and receive activity, as well as traffic that passes through the control plane, use the **show traffic** command in privileged EXEC mode. Packets that go through the control plane path include the control packets for protocols that require Layer 7 inspection as well as management traffic.

show traffic [**detailed** *[type]* | **summary** *[type]*]

Syntax Description

detailed	(Optional) Shows detailed traffic counters for the control plane.
summary	(Optional) Shows traffic summary counters for the control plane.
<i>type</i>	(Optional) Shows the counters for a traffic type. See “ Usage Guidelines ” for a list of traffic types.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The summary and detailed keywords were added.

Usage Guidelines

The **show traffic** command (without any keywords) lists the number of packets and bytes moving through each interface since the last **show traffic** command was entered or since the FWSM came online. The number of seconds shown is the duration the FWSM 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 shown is the duration since that command was entered.

For the **summary** and **detailed** keywords, this command shows the traffic that passes through the control plane, by packet type.

In multiple mode, the system shows cumulative values of all contexts, and the individual contexts show counters for that context only.

Table 30-3 lists the traffic types.

Table 30-3 Traffic Types

Type	Description
activex	ActiveX filtering
all	Shows counters for all transport protocols inspected
ctiqbe	CTIQBE protocol
dns	UDP-based domain name service
domain	TCP-based domain name service
ftp	FTP
ftp-filter	FTP Command filtering
gtp	GTP protocol
h323-h225	H225 protocol
h323-ras	H225 ras protocol
http	HTTP
https-filter	HTTPS protocol filtering
ils	ILS protocol
java	Java filtering
mgcp	MGCP protocol
netbios	NetBIOS protocol
pptp	PPTP
rpc	TCP RPC protocol
rpc-udp	UDP-based RPC protocol
rsh	Remote Shell
rtsp	Real Time Streaming Protocol
sftp	Strict FTP
sip	TCP-based SIP protocol
skinny	Skinny Protocol
smtp	SMTP protocol
snmp	SNMP protocol
sqlnet	SQLNet protocol
sunrpc	TCP-based SunRPC protocol
sunrpc-udp	UDP-based SunRPC protocol
tftp	TFTP
udp-sip	UDP-based SIP protocol
url-filter	URL filtering
xmcp	XDMCP protocol

Examples

The following example shows output from the **show traffic** command:

```
hostname# show traffic
inside:
    received (in 1557469.650 secs):
        157532 packets  13588525 bytes
        0 pkts/sec     0 bytes/sec
    transmitted (in 1557469.650 secs):
        157496 packets  13929928 bytes
        0 pkts/sec     0 bytes/sec
```

The following example shows output from the **show traffic summary** command:

```
hostname# show traffic summary
```

Traffic Type	Pkts-In	Bytes-In	Conn-Created	Conn-Destroyed
url-filter	0	0	0	0
dns	0	0	0	0
activex	0	0	0	0
java	0	0	0	0
domain	0	0	0	0
sftp	0	0	0	0
ftp	0	0	0	0
http	0	0	0	0
h323-h225	0	0	0	0
h323-ras	0	0	0	0
ils	0	0	0	0
sunrpc	0	0	0	0
rpc	0	0	0	0
rsh	0	0	0	0
rtsp	0	0	0	0
smtp	0	0	0	0
sqlnet	0	0	0	0
sip	0	0	0	0
skinny	0	0	0	0
sunrpc-udp	0	0	0	0
rpc-udp	0	0	0	0
xdmcp	0	0	0	0
udp-sip	0	0	0	0
netbios	0	0	0	0
ctiqbe	0	0	0	0
ftp-filter	0	0	0	0
https-filter	0	0	0	0
mgcp	0	0	0	0
tftp	0	0	0	0
snmp	0	0	0	0
pptp	0	0	0	0
gtp	0	0	0	0

The following example shows output from the **show traffic detailed** command:

```
hostname# show traffic detailed
```

```
Traffic Class: url-filter
```

packets received	0
bytes received	0
connections created	0
connections destroyed	0
delete indications received	0
garbage collection initiated connection closure	0

show traffic

```

connections destroyed due to flow handle reuse          0
control channel create requests                         0
data channel create requests                           0
Traffic Class: dns
packets received                                       0
bytes received                                        0
connections created                                    0
connections destroyed                                  0
delete indications received                           0
garbage collection initiated connection closure         0
connections destroyed due to flow handle reuse         0
connections closure initiated from control plane        0
control channel create requests                       0
data channel create requests                           0
....

```

Related Commands	Command	Description
	clear traffic	Resets the counters for transmit and receive activity.

show uauth

To display one or all currently authenticated users (except for management sessions), 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. This command does not show information about management sessions.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **show uauth** command displays the AAA authorization and authentication caches for one user or for all users.

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 FWSM 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 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 FWSM:

```
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:

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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 buffering URLs while waiting for responses 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:

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

Release	Modification
1.1(1)	This command was introduced.

Command History

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 FWSM has looked for a cache entry.
- Hits—The number of times the FWSM 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
```

show url-cache statistics

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 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-server

To display global and individual server information with the URL filtering server, use the **show url-server statistics** command in privileged EXEC mode.

show url-server [statistics]

Syntax Description	statistics Displays global and individual URL server statistics.

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	•	•	•	•	• ¹

1. This command is not supported in the system context when the multiple-context mode is configured.

Command History	Release	Modification
	1.1(1)	This command was introduced.
	3.1(1)	Added the statistics keyword.
	3.2(1)	Changed the format of the CLI output.

Usage Guidelines	The show url-server statistics command displays the URL server vendor; the number of URLs total, allowed, and denied; the number of HTTPs connections total, allowed, and denied; the number of TCP connections total, allowed, and denied; and the URL server status.

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
HTTPs total/allowed/denied 994387/155648/838739
HTTPs allowed by cache/server 70483/85165
HTTPs denied by cache/server 801920/36819
FTPps total/allowed/denied 994387/155648/838739
FTPps allowed by cache/server 70483/85165
FTPps denied by cache/server 801920/36819
Requests dropped 28715
Server timeouts/retries 567/1350
```

show url-server

```

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

```

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 a Smart Filter or Websense server and sets the size of the cache.
url-server	Identifies a Smart Filter 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:

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

Release	Modification
1.1(1)	This command was introduced.

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.



Note

The uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value will continue to increase as long as the other unit continues to operate.

Examples The following example shows how to display the software version, hardware configuration, license key, and related uptime information on a Cisco PIX 500 series FWSM:

```
hostname> show version
Cisco PIX Firewall Version 7.0(1)
PIX (7.0.1.0) #15: Tue XXX 17 14:03:28 EDT 2005
pixfirewall up 5 days 21 hours
Hardware: PIX-515, 96 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash unknown @ 0x0, 0KB
0: Ext: Ethernet0 : media index 0: irq 10
```

```

1: Ext: Ethernet1 : media index 1: irq 7
License Features for this Platform:
Maximum Physical Interfaces : 3
Maximum VLANs : 10
Inside Hosts : Unlimited
Failover : Disabled
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Failover standby only : Disabled
Cut-through Proxy : Enabled
Guards : Enabled
URL-filtering : Enabled
Security Contexts : 0
GTP/GPRS : Disabled
VPN Peers : Unlimited
This machine has a Restricted (R) license.
Serial Number: 12345678
Running Activation Key: 0xbd27f269 0xbc7ebd46 0x1c73e474 0xbb782818 0x071dd0a6
Configuration has not been modified since last system restart.

```

The following example shows how to display the software version, hardware configuration, license key, and related uptime information on a Cisco ASA 5500 series FWSM:

```

hostname# show version
Cisco ASA Software Version 7.0(1)
PIX (7.0.1.0) #28: Mon XXX 23 15:37:25 EDT 2005

ASA up 21 mins 44 secs

Hardware: ASA5530-K8, 2048 MB RAM, CPU Pentium 4 Celeron 2500 MHz
Internal ATA Compact Flash, 489MB
Slot 1: ATA Compact Flash, 244MB
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

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-2.01
0: Ext: GigabitEthernet0/0 : media index 0: irq 9
1: Ext: GigabitEthernet0/1 : media index 1: irq 9
2: Ext: GigabitEthernet0/2 : media index 2: irq 9
3: Ext: GigabitEthernet0/3 : media index 3: irq 9
4: Ext: Management0/0 : media index 0: irq 11
5: Int: No HWIDB : media index 4: irq 11
6: Int: Control0/0 : media index 1: irq 5
License Features for this Platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Enabled
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Cut-through Proxy : Enabled
Guards : Enabled
URL-filtering : Enabled
Security Contexts : 20
GTP/GPRS : Disabled
VPN Peers : 5000
Serial Number: P3000000002
Running Activation Key: 0x881ed361 0x447555a8 0xac73bc44 0xb3f0f888 0x8e26f18b
Configuration register is 0x11
Configuration last modified by enable_15 at 15:55:27.399 UTC Mon XXX 23 2005

```

Related Commands

Command	Description
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the FWSM has been up.

show vlan

To display the system VLANs, use the **show vlan** command in global configuration and 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration and privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you use the **show vlan** command, only VLANs added by the switch are shown.

Examples

The following example displays the system VLANs:

```
hostname(config)# show vlan
10-11, 30, 40, 300
```

Related Commands

Command	Description
clear interface	Clears counters for the show interface command.
clear vlan	Clears the VLANs.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

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}
[filter {name username | ipaddress IPaddr | a-ipaddress IPaddr | p-ipaddress IPaddr |
tunnel-group groupname | protocol protocol-name | encryption encryption-algo}]
[sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]
```

Syntax Descriptions

Granularity of Display

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 FWSM displays the detailed output in a machine-readable format.
filter	Filters the output to display only the information you specify by using one or more of the filter options. For more information, see Usage Guidelines Usage Guidelines.
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 Guidelines Usage Guidelines.

Session Type to Display

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 <i>indexnumber</i>	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 .

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

You can use the following options to filter and to sort the session display:

Filter/Sort Option	Meaning
filter a-ipaddress <i>IPaddr</i>	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 <i>encryption-algo</i>	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 des aes192 3des aes256 rc4
filter ipaddress <i>IPaddr</i>	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 <i>username</i>	Filters the output to display sessions for the specified username(s).
sort name	Sorts the display by usernames in alphabetical order.
filter p-address <i>IPaddr</i>	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 <i>protocol-name</i>	Filters the output to display information for sessions using the specified protocol(s) only.

Filter/Sort Option	Meaning
sort protocol	Sorts the display by protocol. Protocols include: IKE L2TPOverIPSec IMAP4S L2TPOverIPISecOverNatT IPSec POP3S IPSecLAN2LAN PPPoE IPSecLAN2LANOverNatT SMTPS IPSecOverNatT userHTTPS IPSecoverTCP vcaLAN2LAN IPSecOverUDP
filter tunnel-group <i>groupname</i>	Filters the output to display information for the specified tunnel group(s) only.
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 121
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

```

■ show vpn-sessiondb

```

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#
```

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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

show vpn-sessiondb ratio

```
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%
userHTTPS     0            0%
IMAP4S        3 30%
POP3S         0            0%
SMTPS         3 30%
```

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 vpn-sessiondb summary

To display the a summary of current VPN sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode. The session summary includes total current sessions, current sessions of each type, peak and total cumulative sessions, and maximum concurrent sessions.

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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb summary** command:

```
hostname# show vpn-sessiondb summary
```

```
Active Sessions:          Session Information:
  LAN-to-LAN : 2           Peak Concurrent : 7
  Remote Access : 5       Concurrent Limit: 2000
  WebVPN : 0              Cumulative Sessions: 12
  Email Proxy : 0
```

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 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**] [**count**]

Syntax Description

count	(Optional) Displays the translation count.
debug	(Optional) Displays xlate debug information.
detail	(Optional) Displays detail xlate information.
global <i>ip1</i> [- <i>ip2</i>]	(Optional) Displays the active translations by global IP address or range of addresses.
gport <i>port1</i> [- <i>port2</i>]	Displays the active translations by the global port or range of ports.
interface <i>if_name</i>	(Optional) Displays the active translations by interface.
local <i>ip1</i> [- <i>ip2</i>]	(Optional) Displays the active translations by local IP address or range of addresses.
lport <i>port1</i> [- <i>port2</i>]	Displays the active translations by local port or range of ports.
netmask <i>mask</i>	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state <i>state</i>	(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 norandomseq 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 29](#).

Table 30-4 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.

**Note**

When the **vpncient** 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
```

The following sample output from the **show xlate detail** command shows xlate bypass disabled (using the **no xlate bypass** command). The bolded display output shows that all 16 connections require identity NAT xlates even though NAT is not explicitly configured for any of the connections.

```
hostname# show xlate detail
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
16 in use, 16 most used
NAT from inside:10.1.1.11 to outside:10.1.1.11 flags Ii
NAT from inside:10.1.1.12 to outside:10.1.1.12 flags Ii
NAT from inside:10.1.1.13 to outside:10.1.1.13 flags Ii
NAT from inside:10.1.1.14 to outside:10.1.1.14 flags Ii
NAT from inside:10.1.1.15 to outside:10.1.1.15 flags Ii
...
NAT from inside:10.1.1.25 to outside:10.1.1.25 flags Ii
NAT from inside:10.1.1.26 to outside:10.1.1.26 flags Ii.
```

The following sample output from the **show xlate detail** command shows xlate bypass enabled (using the **xlate bypass** command). The bolded display output shows that of the 16 connections active, none require xlates.

```
hostname# show xlate detail
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
0 in use, 16 most used
```

The following sample output from the **show xlate detail** command shows xlate bypass enabled (using the **xlate bypass** command), but includes a static identity NAT configuration, which does require an xlate.

```
hostname(config)# static (inside,outside) 10.1.1.20 10.1.1.20 netmask 255.255.255.255
hostname(config)# show xlate detail
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
1 in use, 16 most used
NAT from inside:10.1.1.20 to outside:10.1.1.20 flags Isi
```


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.



shun through sysopt uauth allow-http-cache 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

<i>dest_port</i>	(Optional) Specifies the destination port of the connection causing the shun.
<i>dst_ip</i>	(Optional) Specifies the address of the target host.
<i>protocol</i>	(Optional) Specifies the IP protocol, such as UDP or TCP. By default, the protocol is 0 (any protocol).
<i>src_ip</i>	Specifies the address of the attacking host.
<i>src_port</i>	(Optional) Specifies the source port of the connection causing the shun.
<i>vlan_id</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM 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 FWSM connection table and also prevents packets from 10.1.1.27:555 to 10.2.2.89:666 (TCP) from going through the FWSM.

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.

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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

Examples

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet2.1
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 gigabitethernet2.1
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.

sip-map

To identify a SIP application inspection map, which is required to enable the IP Address Privacy feature, use the **sip-map** command in global configuration mode. To remove the map, use the **no** form of this command.

sip-map *map_name*

no sip-map *map_name*

Syntax Description

<i>map_name</i>	The name of the SIP map.

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
FWSM 3.1	This command was introduced.

Usage Guidelines

Use the **sip-map** command to identify a SIP application inspection map, which is required to enable the IP Address Privacy feature. When you enter this command, the system enters the SIP map configuration mode, which lets you enter the **ip-address-privacy** command. After defining the SIP map, you use the **inspect sip** 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 SIP traffic, define a SIP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map S1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
hostname(config)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ip-address-privacy	Enables the IP Address Privacy feature for SIP application inspection.
inspect sip	Enables SIP application inspection.
policy-map	Associates a class map with specific security actions.

size

To change the size of a memory partition, use the **size** command in resource partition configuration mode. To restore the size to the default value, use the **no** form of this command.

size *number_of_rules*

no size *number_of_rules*

Syntax Description

number_of_rules Specifies the number of rules you want to assign to the partition.

Defaults

The default size of a partition depends on the total number of partitions. To view the default partition sizes, enter the **show resource partition** command.

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
4.0(1)	This command was introduced.

Usage Guidelines

The FWSM lets you set the memory size of each partition. See the following guidelines before you change partition sizes:

- Changing the partition sizes requires you to reload the FWSM.
- Change the number of partitions before you set the partition sizes using the **resource acl-partition** command; changing the number of partitions affects the overall number of rules per partition. If you increase the number of partitions, for example, then the number of rules available per partition will be smaller. Therefore, your partition size configuration might be invalid, and you might need to reconfigure all your partition sizes. Changing the number of partitions requires you to reload the FWSM before you change the partition sizes; then changing the partition sizes requires a second reload.
- Allocate contexts to specific partitions before you set the partition sizes (see the **allocate-acl-partition** command). If you plan all your partition sizes based on the contexts currently assigned to a partition, but you did not specifically allocate the contexts, then you run the risk of context assignments shifting after a reload (for example if you add or subtract contexts).
- Reduce the size of partition(s) before increasing the size of other partition(s).
- If the existing number of ACEs does not fit into the new partition size, then the resizing is rejected.

- In addition to the memory partitions to which the FWSM assigns contexts, the FWSM uses a backup tree partition to process changes to rules so traffic can continue to use the old configuration until the new configuration is ready. The backup tree must be as large as the largest partition. Therefore, some memory is automatically assigned to the backup tree in tandem with the largest partition; so be sure to include the backup tree in your calculations.
- If you reduce the size of a partition, the FWSM checks the rule allocation (see the **resource rule** or **rule** command). If you manually allocated rules between features so that the total number of rules allocated is now greater than those available, then the FWSM rejects the resizing of the partition. Similarly, if the absolute maximum number of rules for a feature is now exceeded, then the FWSM rejects the resizing of the partition.

To view the rules available for increasing partition sizes, enter the **show resource partition** command.

For example, if you reduced the sizes of partitions 0 through 5 to 15,000, then the output shows that you have 25,314 rules to reallocate to other partitions.

```
hostname(config)# show resource partition
```

Partition Number	Default Size	Bootup Partition Size	Current Configured Size
0	19219	19219	15000
1	19219	19219	15000
2	19219	19219	15000
3	19219	19219	15000
4	19219	19219	15000
5	19219	19219	15000
6	19219	19219	19219
7	19219	19219	19219
8	19219	19219	19219
9	19219	19219	19219
10	19219	19219	19219
11	19219	19219	19219
backup tree	19219	19219	19219
Total	249847	249847	224533

```
Total Partition size - Configured size = Available to allocate
249847 - 224533 = 25314
```

If you want to distribute the rules evenly across the other 6 partitions plus the backup tree, then you can add 3616 rules to each (with 2 left over). Remember that the backup tree must be as large as the largest partition, so you must consider the backup tree in your calculations. For example, if you want to make partition 6 have 24,001 rules, then you can allocate the rules like this:

Partition	Bootup Partition Size	Configured Size	Difference
6	19219	24001	4782
Backup Tree	19219	24001	4782
7	19219	22369	3150
8	19219	22369	3150
9	19219	22369	3150
10	19219	22369	3150

Partition	Bootup Partition Size	Configured Size	Difference
11	19219	22369	3150
			Total: 25314

You can also view the current mapping of contexts to partitions using the **show resource acl-partition** command.

Examples

The following example reduces partitions 0 and 1 to 40000, while increasing partitions 2 and 3 to 56616 and 56615 respectively.

```
hostname(config)# show resource partition
```

Partition Number	Default Size	Bootup Partition Size	Current Configured Size
0	49970	49970	49970
1	49969	49969	49969
2	49969	49969	49969
3	49969	49969	49969
backup tree	49970	49970	49970
Total	249847	249847	249847

```
Total Partition size - Configured size = Available to allocate
249847 - 249847 = 0
```

```
hostname(config)# resource partition 0
hostname(config-partition)# size 40000
hostname(config-partition)# resource partition 1
hostname(config-partition)# size 40000
```

```
hostname(config-partition)# show resource partition
```

Partition Number	Default Size	Bootup Partition Size	Current Configured Size
0	49970	49970	40000
1	49969	49969	40000
2	49969	49969	49969
3	49969	49969	49969
backup tree	49970	49970	49969
Total	249847	249847	249847

```
Total Partition size - Configured size = Available to allocate
249847 - 229907 = 19940
```

```
hostname(config-partition)# resource partition 2
hostname(config-partition)# size 56616
hostname(config-partition)# resource partition 3
hostname(config-partition)# size 56615
```

```
hostname(config-partition)# show resource partition
```

Partition Number	Default Size	Bootup Partition Size	Current Configured Size

size

```

-----+-----+-----+-----
      0      49970      49970      40000
      1      49969      49969      40000
      2      49969      49969      56616
      3      49969      49969      56615
backup tree 49970      49970      56616
-----+-----+-----+-----
      Total      249847      249847      249847

```

```

Total Partition size - Configured size = Available to allocate
      249847 -      249847 =      0

```

```
hostname(config-partition)# reload
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource partition	Shows the memory partition sizes.
show resource rule	Shows the current allocation of rules.
show running-config resource partition	Shows the current memory partition configuration.

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 FWSM 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 on the FWSM.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

Syntax Description

<i>primary_server</i>	Identifies the primary SMTP server. Use either an IP address or DNS name
<i>backup_server</i>	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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

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:

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

Command History

Release	Modification
3.1(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)# exit
```

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.
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

By default, the community string is **public**.

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
1.1(1)	This command was introduced.

Usage Guidelines

The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. The FWSM uses the key to determine if the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the routers, FWSM, and the management station with this same string. The FWSM 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 FWSM.
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 contact name, use the **snmp-server contact** command in global configuration mode. To remove the 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 FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example sets the 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 FWSM.
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 FWSM, use the **snmp-server enable** command in global configuration mode. To disable SNMP, use the **no** form of this command.

snmp-server enable

no snmp-server enable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the SNMP server is enabled.

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
3.1(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 FWSM 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*] [...] | **cpu threshold** [*trap*] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **nat** [*trap*] | **remote-access** [*trap*] | **resource** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **cpu threshold** [*trap*] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **nat** [*trap*] | **remote-access** [*trap*] | **resource** [*trap*]]

Syntax Description	
all	Enables all traps.
cpu threshold [<i>trap</i>]	Enables CPU threshold traps. Traps for cpu threshold include: • rising
entity [<i>trap</i>]	Enables entity traps. Traps for entity include: • config-change • fru-insert • fru-remove • redun-switchover • alarm-asserted • alarm-cleared
ipsec [<i>trap</i>]	Enables IPSec traps. Traps for ipsec include: • start • stop
nat [<i>trap</i>]	Enables NAT-related traps. Traps for nat include: • packet-discard
remote-access [<i>trap</i>]	Enables remote access traps. Traps for remote-access include: • session-threshold-exceeded
resource [<i>trap</i>]	Enables resource limit traps. Traps for resource include: • limit-reached • rate-limit-reached
snmp [<i>trap</i>]	Enables SNMP traps. By default, all SNMP traps are enabled. Traps for snmp include: • authentication • linkup • linkdown • coldstart
syslog	Enables syslog 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		
	Routed	Transparent	Single	Multiple	
				Context	Administrative
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	Added cpu threshold trap: <i>rising</i> . Added entity traps: <i>redun-switchover</i> , <i>alarm-asserted</i> , and <i>alarm-cleared</i> . Added nat trap: <i>packet-discard</i> . Added resource traps: <i>limit-reached</i> and <i>rate-limit-reached</i> .
4.0(1)	The remote-access option in multi-firewall mode was removed.

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.

The **remote-access** option is not available in multi-firewall mode in FWSM Version 4.0

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 FWSM.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server host

To specify the NMS that can use SNMP on the FWSM, use the **snmp-server host** command in global configuration mode. To disable the NSM, use the **no** form of this command.

snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community text**] [**version {1 | 2c}**]
[**udp-port port**]

no snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community text**] [**version {1 | 2c}**]
[**udp-port port**]

Syntax Description

community text	Sets the community string for this NMS.
host	Specifies an IP address of the NMS to which traps should be sent or from which SNMP requests come.
<i>interface_name</i>	Specifies the interface name through which the NMS communicates with the FWSM.
<i>ip_address</i>	Specifies the IP address of an NMS to which SNMP traps should be sent or from which the SNMP requests come.
trap	(Optional) Specifies that only traps are sent, and that this host is not allowed to browse (poll).
poll	(Optional) Specifies that this host is allowed to browse (poll), but no traps are sent.
udp-port udp_port	(Optional) Sets the UDP port to which notifications are sent. SNMP traps are sent on UDP port 162 by default.
version {1 2c}	(Optional) Sets the SNMP notification version to version 1 or 2c.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can specify up to 32 NMSs.

Examples

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
```

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 FWSM.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server listen-port

To set the listen 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	<i>lport</i>	The port on which incoming requests will be accepted. The default port is 161.

Defaults	The default port is 161.

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
	1.1(1)	This command was introduced.

Examples	The following example sets the listen port to 192:
	<code>hostname(config)# snmp-server listen-port 192</code>

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 FWSM.
	snmp-server enable traps	Enables SNMP traps.
	snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example sets the location 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 FWSM.
snmp-server enable traps	Enables SNMP traps.
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:

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

Command History

Release	Modification
4.0(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.

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.

split-dns { **value** *domain-name1 domain-name2 domain-nameN* | **none** }

no split-dns [*domain-name domain-name2 domain-nameN*]

Syntax Description

value <i>domain-name</i>	Provides a domain name that the FWSM 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:

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

Command History

Release	Modification
3.1(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 (.).

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.

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 the IPsec client uses 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 FWSM 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:

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

Command History

Release	Modification
4.0(1)	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 Vlan10:

```
hostname(config)# interface Vlan10
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.

split-tunnel-network-list {**value** *access-list name* | **none**}

no split-tunnel-network-list value [*access-list name*]

Syntax Description

value <i>access-list name</i>	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 FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM 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.

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.

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 the IPsec client uses 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-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 FWSM. 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 Internet service provider of the remote user.

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:

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

Command History

Release	Modification
3.1(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. 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.

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 the IPSec client uses 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 FWSM uses to distinguish networks that require tunneling and those that do not.

ssh

To add SSH access to the FWSM, use the **ssh** command in global configuration mode. To disable SSH access to the FWSM, 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

<i>interface</i>	The FWSM interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface.
<i>ip_address</i>	IPv4 address of the host or network authorized to initiate an SSH connection to the FWSM. For hosts, you can also enter a host name.
<i>ipv6_address/prefix</i>	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the FWSM.
<i>mask</i>	Network mask for <i>ip_address</i> .

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	Support for this command was introduced.

Usage Guidelines

The **ssh ip_address** command specifies hosts or networks that are authorized to initiate an SSH connection to the FWSM. 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 FWSM, you must generate a default RSA key using the **crypto key generate rsa** command.

The following security algorithms and ciphers are supported on the FWSM:

- 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 FWSM:

- 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 FWSM.
ssh version	Restricts the FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM.
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh scopy enable

To enable Secure Copy (SCP) on the FWSM, 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:

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

Release	Modification
3.1(1)	Support for this command was introduced.

Command History

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 FWSM has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the FWSM internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The FWSM license must have the VPN-3DES-AES feature to support SSH version 2 connections.

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 FWSM from the specified client or network.
ssh version	Restricts the FWSM 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

<i>number</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM.
ssh disconnect	Disconnects an active SSH session.

ssh version

To restrict the version of SSH accepted by the FWSM, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command.

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:

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

1 and 2 specify which version of SSH the FWSM is restricted to using. The **no** form of the command returns the FWSM to the default stance, which is compatible mode (both version can be used). The default values permit SSH Version 1 and SSH Version 2 connections to the FWSM.

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.

Command	Description
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the FWSM from the specified client or network.

ssl server-version

To specify the SSL/TLS protocol version FWSM 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/TLS that FWSM accepts.

ssl server-version [*any* | *ssl3* | *tlsv1* | *ssl3-only* | *tlsv1-only*]

no ssl server-version

Syntax Description

<i>any</i>	Accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
<i>ssl3</i>	Accepts SSL version 2 client hellos, and negotiates to SSL version 3.
<i>ssl3-only</i>	Accepts only SSL version 3 client hellos, and uses only SSL version 3.
<i>tlsv1</i>	Accepts SSL version 2 client hellos, and negotiates to TLS version 1.
<i>tlsv1-only</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **ssl server-version** command to enforce what version of SSL is accepted when HTTPS clients connect directly to the firewall for management of the firewall. On the FWSM, the command does not support the WebVPN feature.

Examples

The following example shows how to configure FWSM to communicate using only TLSv1 when acting as an SSL server:

```
hostname(config)# ssl server-version tlsv1-only
```


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:

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

Command History

Release	Modification
4.0(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]
```

```
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]
```

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]
```

```
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]
```

Syntax Description

access-list <i>access_list_name</i>	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 destination 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: <pre>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</pre> 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 FWSM 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.
<i>emb_lim</i>	(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 FWSM 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. 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.
<i>mapped_ifc</i>	Specifies the name of the interface connected to the mapped IP address network.
<i>mapped_ip</i>	Specifies the address to which the real address is translated.
<i>mapped_port</i>	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

netmask <i>mask</i>	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 <i>real_ip</i> , then the subnet mask used in the access list is also used for the <i>mapped_ip</i> .
norandomseq	(Optional) Disables TCP ISN randomization protection. TCP initial sequence number randomization can be disabled if another in-line firewall is also randomizing the initial sequence numbers, because there is no need for both firewalls to be performing this action. However, leaving ISN randomization enabled on both firewalls does not affect the traffic. 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 the outbound direction. If the connection is between two interfaces with the same security level, then the ISN will be randomized in the SYN in both 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. The norandomseq keyword does not apply to outside NAT. The firewall randomizes only the ISN that is generated by the host/server on the higher security interface. If you set norandomseq for outside NAT, the norandomseq keyword is ignored.
<i>real_ifc</i>	Specifies the name of the interface connected to the real IP address network.
<i>real_ip</i>	Specifies the real address that you want to translate.
<i>real_port</i>	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 <i>max_conns</i>	Specifies the maximum number of simultaneous TCP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the timeout conn command.)
udp	For static PAT, specifies the protocol as UDP.
udp <i>udp_max_conns</i>	(Optional) Specifies the maximum number of simultaneous UDP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the timeout conn command.)

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.2.(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).

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.

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 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, and so on.), the FWSM automatically translates the secondary ports.

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 FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the FWSM 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.

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
```

The following 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
```

The following 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 should 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 FWSM 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 10.1.3.0 255.255.255.0 eq
telnet
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 FWSM 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 10.1.3.0 255.255.255.0 eq
http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the FWSM 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:

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

Command History	Release	Modification
	4.0(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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the FWSM 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
```

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 FWSM selects the tunnel group for PPP connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the FWSM sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPsec remote access and L2TP/IPsec 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-general)# default-group-policy remotegrp
hostname(config-general)# strip-group
hostname(config-general)
```

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-map default group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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 FWSM sends only the user part of the username authorization/authentication. Otherwise, the FWSM 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:

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

Command History

Release	Modification
3.1(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-general)# default-group-policy remotegrp
hostname(config-general)# strip-realm
```

neral)

ostname(config-ge

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-limit	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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 CA certificate map configuration mode. To remove a 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	Optional) 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 the DN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
<i>string</i>	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
3.1(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
hostname(config)#
```

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

<i>X.500_name</i>	Defines the X.500 distinguished name, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum length is 1K characters (effectively unbounded).

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:

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

Command History

Release	Modification
3.1(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://www.example.com and includes the subject DN OU cisco.example in the the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://www.example.com/
hostname(ca-trustpoint)# subject-name ou=cisco.example
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.

summary-address eigrp

To configure a summary for EIGRP on a specific interface, use the **summary-address eigrp** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

summary-address eigrp *as-number addr mask [admin-distance]*

no summary-address *as-number addr mask*

Syntax Description

<i>as-number</i>	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.
<i>addr</i>	The summary IP address.
<i>mask</i>	The subnet mask to apply to the IP address.
<i>admin-distance</i>	(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:

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

Command History

Release	Modification
4.0(1)	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 eigrp** 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.

summary-address

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

<i>addr</i>	Value of the summary address that is designated for a range of addresses.
<i>mask</i>	IP subnet mask that is used for the summary route.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair.
tag <i>tag_value</i>	(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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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	Displays the summary address settings for each OSPF routing process.
summary-address	

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

<i>ifc_name</i>	Server interface name.
<i>ip_addr</i>	SunRPC server IP address.
<i>mask</i>	Network mask.
port <i>port</i> [- <i>port</i>]	Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service <i>service_type</i>	Sets the SunRPC service program number as specified in the output of a SunOS rpcinfo command.
timeout <i>hh:mm:ss</i>	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:

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

Command History

Release	Modification
2.2(1)	The rpc-server command was introduced.
3.1(1)	This command was changed from rpc-server .

Usage Guidelines

The SunRPC services table is used to allow SunRPC traffic through the FWSM 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 FWSM.
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:

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines The FWSM 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.

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

<i>bytes</i>	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 <i>bytes</i> to 0. For the minimum keyword, the <i>bytes</i> represent the smallest maximum value allowed.
minimum	(Optional) Overrides the maximum segment size to be no less than <i>bytes</i> , 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM 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 FWSM alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the FWSM 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 FWSM 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 FWSM 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 timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP for global addresses, use the **no** form of this command.

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

Syntax Description

interface_name Specifies the interface name for which you want to disable proxy ARP.

Defaults

Proxy ARP for global addresses 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

In rare circumstances, you might want to disable proxy ARP for 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 FWSM uses proxy ARP when you configure NAT and specify a global address that is on the same network as the FWSM interface. The only way traffic can reach the hosts is if the FWSM uses proxy ARP to claim that the FWSM 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Some RADIUS servers, such as Livingston Version 1.16, have a usage caveat where they do not include the key in the authenticator hash in the accounting acknowledgment response. This situation can cause the FWSM to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in the authenticator of accounting acknowledgments thus avoiding the retransmit problem. (The key described here is the key 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.

sysopt uauth allow-http-cache

To let the web browser supply a username and password from its cache when it reauthenticates with the virtual HTTP server on the FWSM (see the **virtual http** command), use the **sysopt uauth allow-http-cache** command in global configuration mode. If you do not allow the HTTP cache, then after your authentication session times out, the next time you connect to the virtual HTTP server, you are prompted again for your username and password. To disable this feature, use the **no** form of this command.

sysopt uauth allow-http-cache

no sysopt uauth allow-http-cache

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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example allows the HTTP cache to be used:

```
hostname(config)# sysopt uauth allow-http-cache
```

Related Commands

Command	Description
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command allows you to authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
clear configure sysopt	Clears the sysopt command configuration.
show running-config sysopt	Shows the sysopt command configuration.



CHAPTER

32

telnet through tunnel-limit Commands

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

<i>hostname</i>	Specifies the name of a host that can access the Telnet console of the FWSM.
<i>interface_name</i>	Specifies the name of the network interface to Telnet to.
<i>IP_address</i>	Specifies the IP address of a host or network authorized to log in to the FWSM.
<i>IPv6_address</i>	Specifies the IPv6 address/prefix authorized to log in to the FWSM.
<i>mask</i>	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 FWSM; valid values are from 1 to 1440 minutes.

Defaults

By default, Telnet sessions left idle for five minutes are closed by the FWSM.

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
3.1(1)	The variable <i>IPv6_address</i> was added. The no telnet timeout command was added.

Usage Guidelines

The **telnet** command lets you specify which hosts can access the FWSM console with Telnet. You can enable Telnet to the FWSM on all interfaces. However, the FWSM 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 FWSM 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 FWSM. 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 subnet 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 FWSM 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 FWSM Telnet console access and the console login request times out, you can gain access to the FWSM from the serial console by entering the FWSM 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 FWSM 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
```

show 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 FWSM.
who	Displays active Telnet administration sessions on the FWSM.

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 on the current Telnet session.
no monitor	Disables the display of system log messages on 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

This example shows how to enable logging and then disable logging only 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:

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

Command History

Release	Modification
3.1(1)	This command was changed from the pager command; the pager command is now a global configuration mode command.

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 or session to the system execution space, 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.
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messages 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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM 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 FWSM, 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 <i>ip_address</i>	Specifies the server IP address. If you do not specify the IP address in the command, you are prompted for it.
password <i>password</i>	Specifies the user password. If you do not specify the password in the command, you are prompted for it.
<i>server_tag</i>	Specifies the AAA server tag as set by the aaa-server command.
username <i>username</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **test aaa-server** command lets you verify that the FWSM 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 FWSM.

Examples

The following example configures a RADIUS AAA server named `svrgrp1` 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 regex

To test a regular expression, use the **test regex** command in privileged EXEC mode.

test regex *input_text* *regular_expression*

Syntax Description

<i>input_text</i>	Specifies the text that you want to match with the regular expression.
<i>regular_expression</i>	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:

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

Command History

Release	Modification
4.0(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.

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

<i>interface_name</i>	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.
<i>server</i>	Sets the TFTP server IP address or name. You can enter an IPv4 or IPv6 address.
<i>filename</i>	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:

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

Command History

Release	Modification
3.1(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 FWSM supports only one **tftp-server** command.



Note

With the **tftp-server** command configured to define an interface, the **copy** command will attempt to copy files from the interface specified. You can override that interface in the **copy** command using the **int** keyword.

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.

timeout

To set the maximum idle time duration, use the **timeout** command in global configuration mode.

timeout { **xlate** | **conn** | **half-closed** | **udp** | **icmp** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **non_tcp_udp** | **sunrpc** | **uauth** } *hh:mm:ss*

Syntax Description

conn	Specifies the idle time after which a connection closes; the minimum duration is five minutes.
<i>hh:mm:ss</i>	Specifies the timeout.
h225	Specifies the idle time after which an H.225 signaling connection closes.
h323	Specifies the idle time after which H.245 (TCP) and H.323 (UDP) media connections close. The default is five minutes.
 Note	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	Specifies the idle time after which a TCP half-closed connection will be freed.
icmp	Specifies the idle time for ICMP.
mgcp	Sets the idle time after which an MGCP media connection is removed.
mgcp-pat	Sets the absolute interval after which an MGCP PAT translation is removed.
non_tcp_udp	Sets the idle time after which an non TCP/UDP connection will be closed.
sip	Modifies the SIP timer.
sip-disconnect	Sets the idle time after which media is deleted and media xlates are closed. Range is from 1 to 10 minutes. Default is 2 minutes.
sip-invite	Sets the idle time after which pinholes for provisional responses and media xlates are closed. Range is from 1 to 30 minutes. Default is 3 minutes.
sip_media	Modifies the SIP media timer, which is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
sunrpc	Specifies the idle time after which a SUNRPC slot will be closed.
uauth	Sets the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection.
udp	Specifies the idle time until a UDP slot is freed; the minimum duration is one minute.
xlate	Specifies the idle time until a translation slot is freed; the minimum value is one minute.

Defaults

The defaults are as follows:

- **conn** *hh:mm:ss* is 1 hour (**01:00:00**).
- **h225** *hh:mm:ss* is 1 hour (**01:00:00**).
- **h323** *hh:mm:ss* is 5 minutes (**00:05:00**).
- **half-closed** *hh:mm:ss* is 10 minutes (**00:10:00**).

- **icmp** *hh:mm:ss* is 2 minutes (**00:00:02**).
- **mgcp** *hh:mm:ss* is 5 minutes (**00:05:00**).
- **mgcp-pat** *hh:mm:ss* is 5 minutes (**00:05:00**).
- **non_tcp_udp** *hh:mm:ss* is 10 minutes (**00:10:00**).
- **sip** *hh:mm:ss* is 30 minutes (**00:30:00**).
- **sip-disconnect** *hh:mm:ss* is 2 minutes (**00:02:00**).
- **sip-invite** *hh:mm:ss* is 3 minutes (**00:03:00**).
- **sip_media** *hh:mm:ss* is 2 minutes (**00:02:00**).
- **sunrpc** *hh:mm:ss* is 10 minutes (**00:10:00**).
- **uauth** timer is **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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	The keyword mgcp-pat was added. The rpc keyword was changed to sunrpc .
3.2(1)	The keywords sip-disconnect and sip-invite were added.

Usage Guidelines

The **timeout** command lets you set the idle time for many processes. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.



Note

Do not use the **timeout uauth 0:0:0** command if passive FTP is used for the connection or if the **virtual** command is used for web authentication.

The connection timer takes precedence over the translation timer; the translation timer works only after all connections have timed out.

When setting the **conn hh:mm:ss**, use **0:0:0** to never time out a connection.

When setting the **half-closed hh:mm:ss**, use **0:0:0** to never time out a half-closed connection.

When setting the **h255** *hh:mm:ss*, **h225 00:00:00** means to never tear down an H.225 signaling connection. A timeout value of **h225 00:00:01** disables the timer and closes the TCP connection immediately after all calls are cleared.

The **uauth** *hh:mm:ss* duration must be shorter than the **xlite** keyword. Set to **0** to disable caching. Do not set to zero if passive FTP is used on the connections.

To disable the **absolute** keyword, set the uauth timer to **0** (zero).

Examples

The following example shows how to configure the maximum idle time durations:

```
hostname(config)# timeout uauth 0:5:00 absolute uauth 0:4:00 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
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 FWSM gives up on the request to the primary AAA server. If there is a standby AAA server, the FWSM 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:

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

Command History

Release	Modification
3.1(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 FWSM attempts to make a connection to a AAA server. Use the **retry-interval** command to specify the amount of time the FWSM waits between connection attempts.

The timeout is the total amount of time that the FWSM 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 must be less than the 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 FWSM 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)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa server host configuration mode so that 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 (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** | **tunnel** } *hh:mm:ss*

no timeout { **gsn** | **pdp-context** | **request** | **signaling** | **tunnel** } *hh:mm:ss*

Syntax Description

<i>hh:mm:ss</i>	This is the timeout where <i>hh</i> specifies the hour, <i>mm</i> specifies the minutes, and <i>ss</i> specifies the seconds. 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.
tunnel	Specifies the 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 minute (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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The PDP context is identified by the 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 pinhole

To configure the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes, use the **timeout pinhole** command in dcerpc-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:

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

Command History

Release	Modification
3.2(1)	This command was introduced.

Examples

The following example shows how to configure the pinhole timeout for pin hole connections in a DCERPC inspection map:

```
hostname(config)# dcerpc_map dmap
hostname(config-dcerpc-map)# timeout pinhole 0:10:00
```

Related Commands

Command	Description
clear configure dcerpc-map	Clears DCERPC map configuration.
endpoint-mapper	Configures options for the endpoint mapper traffic.
show running-config dcerpc-map	Display all current DCERPC 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:

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

Command History

Release	Modification
3.1(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 FWSM; 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 FWSM.
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.

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

<i>seconds</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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

<i>delay</i>	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.
<i>holdtime</i>	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:

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

Command History

Release	Modification
1.1(1)	This command was introduced.

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.

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 disabled 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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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 FWSM 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		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable the **transfer-encoding** command, the FWSM applies the specified action to HTTP connections for each supported and configured transfer encoding type.

The FWSM 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 FWSM 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
```

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
```

In this case, only connections using no transfer encoding are allowed. When HTTP traffic for the other supported encoding types is received, the FWSM 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all 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-ipsec)# trust-point mytrustpoint
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
crypto ca trustpoint	Enters the trustpoint mode for the specified trustpoint.

Command	Description
show running-config tunnel-group	Shows the configuration for the indicated tunnel group or for all tunnel groups.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

tunnel-group

To create and manage the database of connection-specific records for IPSec, 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

<i>name</i>	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.
<i>type</i>	Specifies the type of tunnel group: L2TP/IPSec— L2TP over IPSec ipsec-ra—IPSec remote access ipsec-l2l—IPsec LAN-to-LAN

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	•	•	•	•	—



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. All the tunnel-group commands that are available for LAN-to-LAN are also available in transparent firewall mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM has two default tunnel groups: DefaultRAGroup, which is the default IPSec remote-access tunnel group, and DefaultL2Lgroup, which is the default IPSec LAN-to-LAN tunnel group. You can change them but not delete them. The FWSM 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.

The **tunnel-group** command has the following commands. Each of these commands puts you in a configuration mode for configuring the attributes at the level of the configuration mode.

- **tunnel-group general-attributes**

- tunnel-group ipsec-attributes
- tunnel-group ppp-attributes

Examples

The following example entered in global configuration mode, configures an IPSec LAN-to-LAN tunnel group. The name is the IP address of the LAN-to-LAN peer:

```
hostname(config)# tunnel-group 209.165.200.225 type ipsec-l2l  
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 map	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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.
<i>name</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The following table lists the commands belonging in this group and the tunnel-group type where you can configure them:

General Attribute	Availability by Tunnel-Group Type
accounting-server-group	IPSec RA, IPSec L2L, L2TP/IPSec
address-pool	IPSec RA, L2TP/IPSec
authentication-server-group	IPSec RA, L2TP/IPSec
authorization-server-group	IPSec RA, L2TP/IPSec
default-group-policy	IPSec RA, IPSec L2L, L2TP/IPSec
dhcp-server	IPSec RA, L2TP/IPSec
strip-group	IPSec RA, L2TP/IPSec
strip-realm	IPSec RA, L2TP/IPSec

Examples

The following example entered in global configuration mode, creates a tunnel group for an IPSec LAN-to-LAN connection using the IP address of the LAN-to-LAN peer, then enters general configuration mode for configuring general attributes. The name of the tunnel group is 209.165.200.225.

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 general
hostname(config-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-general)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the configuration for the indicated tunnel group or for all tunnel groups.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

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.
<i>name</i>	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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The following commands belong in this group:

IPSec Attribute	Availability by Tunnel-Group Type
authorization-dn-attributes	IPSec RA
authorization-required	IPSec RA
chain	IPSec RA, IPSec L2L, L2TP/IPSec
client-update	IPSec RA
isakmp keepalive	IPSec RA
peer-id-validate	IPSec RA, IPSec L2L, L2TP/IPSec
pre-shared-key	IPSec RA, IPSec L2L, L2TP/IPSec
radius-with-expiry	IPSec RA
trust-point	IPSec RA, IPSec L2L, L2TP/IPSec

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-ipsec)
```

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-group-map default-group

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.

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 [*rule-index*] **default-group** *tunnel-group-name*

Syntax Description

default-group	Specifies a default tunnel group to use when the name cannot be derived by other configured methods. The <i>tunnel-group name</i> must already exist.
<i>tunnel-group-name</i>	
<i>rule index</i>	(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:

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

Command History

Release	Modification
3.1(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.

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 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

The **tunnel-group-map enable** command in global configuration mode 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 [*rule-index*] **enable** *policy*

Syntax Description

<i>policy</i>	Specifies the policy for deriving the tunnel group name from the certificate. <i>Policy</i> 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 organizational unit (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.
<i>rule index</i>	(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:

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

Command History

Release	Modification
3.1(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-limit

To specify the maximum number of GTP tunnels allowed to be active on the FWSM, 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(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 gtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

Related Commands

Commands	Description
clear service-policy	Clears global GTP statistics.
inspect gtp	
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.



upgrade-mp through xlate-bypass Commands

upgrade-mp

To upgrade the maintenance partition software, use the **upgrade-mp** command.

```
upgrade-mp {http[s]://[user:password@]server[:port]/pathname | tftp[://server/pathname]}
```

Syntax Description

tftp	Specifies a TFTP server. If you do not specify the server and path, you are prompted for the information. See the tftp-server command to configure a default TFTP server.
http[s]	Specifies an HTTP(S) server.
<i>server</i>	Specifies the HTTP(S) or TFTP server IP address.
<i>pathname</i>	Specifies the pathname and filename of the software image.
<i>user</i>	(Optional) Specifies the HTTP(S) username.
<i>password</i>	(Optional) Specifies the user password.
<i>port</i>	(Optional) Specifies the HTTP(S) port.

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
Privileged mode	•	•	•	—	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example shows how to download an image from a TFTP server:

```
hostname# upgrade-mp tftp://10.192.1.1/c6svc-mp.2-1-1.bin.gz
```

Related Commands

Command	Description
copy	Copies a file to Flash memory.

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
4.0(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

<i>index</i>	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The FWSM tries the URL at index 1 first.
<i>url</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
CRL configure configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	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 **crl configure** configuration mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL <https://example.com> from which to retrieve CRLs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://example.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 in global configuration mode. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer_limit*

no url-block block *block_buffer_limit*

Websense only:

url-block url-mempool *memory_pool_size*

no url-block url-mempool *memory_pool_siz*

Syntax Description

block <i>block_buffer_limit</i>	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. In single context mode, the permitted values are from 0 to 128, which specifies the number of 1550-byte blocks. In multiple context mode, the permitted values are from 0 to 16.
url-mempool <i>memory_pool_size</i>	For Websense URL filtering only. The size of the URL buffer memory pool in Kilobytes (KB). In single context mode, the permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB. In multiple context mode, the permitted values are from 0 to 512.
url-size <i>long_url_size</i>	For Websense URL filtering only. The maximum allowed URL size in KB. The permitted values are 2, 3, or 4, which specifies a maximum URL size of 2 KB, 3 KB, or 4 KB.

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

For Websense filtering servers, the **url-block url-size** command allows filtering of long URLs, up to 4 KB. For both Websense and N2H2 filtering servers, the **url-block block** command causes the FWSM 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 FWSM 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 FWSM 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 FWSM 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 url-mempool** command to specify the maximum length of a URL to be filtered by a Websense filtering server 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 server. The **url-block url-size** command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense server (through a TCP packet stream) so that the Websense 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 block, 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 while pending responses from an N2H2 or 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 N2H2 or Websense server.
kb	(Optional) Indicates that the size given is in kilobytes. FWSM accepts the kb keyword as a convenience in case you add it as a habit.
<i>kbytes</i>	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 N2H2 or 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **url-cache** command provides a configuration option to buffer the response from a web server if its response is faster than that from the N2H2 or Websense filtering service server. This prevents the web server response from being loaded twice.

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 FWSM. When a host requests a connection, the FWSM first looks in the URL cache for matching access privileges instead of forwarding the request to the N2H2 or Websense server. Disable caching with the **no url-cache** command.

**Note**

If you change settings on the N2H2 or Websense server, disable the cache with the **no url-cache** command and then reenable 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 that 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 and for N2H2 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 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-server

To identify a smartfilter (formerly 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.

smartfilter (formerly 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 1|4][context-name]
```

```
no url-server (if_name) vendor websense host local_ip [timeout seconds] [protocol {TCP | UDP | connections num_conns} | version 1|4][context-name]
```

Syntax Description

smartfilter (formerly N2H2)

connections <i>num_conns</i>	Indicates number of simultaneous TCP connections established between URL-server and the FWSM. Default value is 5.
host <i>local_ip</i>	The server that runs the URL filtering application.
<i>if_name</i>	The network interface where the authentication server resides.
port <i>number</i>	The smartfilter (formerly N2H2) server port. The FWSM 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 <i>seconds</i>	The idle time permitted before the server is marked down and the FWSM switches to the next server, if specified. Default timeout is 30 seconds.
vendor smartfilter (formerly N2H2)	Indicates URL filtering service vendor is smartfilter (formerly N2H2).

Websense

connections <i>num_conns</i>	Indicates number of simultaneous TCP connections established between URL-server and the FWSM. Default value is 5.
context-name	Sends the context name with each websense query for policy lookups on the websense server.
 Note This feature is available only when websense is configured for filtering [not available with smartfilter (formerly N2H2)], and with websense protocol version 4.0. This feature can be configured only in multiple context mode.	
<i>if_name</i>	The network interface where the authentication server resides.
host <i>local_ip</i>	The server that runs the URL filtering application.
timeout <i>seconds</i>	The idle time permitted before the server is marked down and the FWSM switches to the next server, if specified. Default timeout 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.
<i>version</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
4.0	Introduced the context-name feature.

Usage Guidelines

The **url-server** command designates the server running the smartfilter (formerly N2H2) or Websense URL filtering application. The limit is 16 URL servers; however, you can use only one application at a time, either smartfilter (formerly N2H2) or Websense. Additionally, changing your configuration on the FWSM 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 URL, HTTPS and FTP filtering. Before removing all the url-servers from the server list, associated filter commands must be removed.

Once you designate the server, enable the filtering service with the **filter url** command.

To filter URLs, perform the following steps:

-
- 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 smartfilter (formerly N2H2), visit the smartfilter (formerly N2H2) website at:

<http://www.n2h2.com>



Note

The N2H2 corporation was acquired by Secure Computing in October, 2003.

For more information on Websense filtering services, visit the following website:

<http://www.websense.com/>

Examples

Using smartfilter (formerly 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) 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
```

Using Websense, the following example uses the context-name feature:

```
url-server (inside) host 10.1.1.10 protocol TCP version 4 connections 5 context-name
url-server (inside) host 10.1.1.10 timeout 20 protocol UDP version 4 context-name
```

Related Commands

Commands	Description
show url-server statistics	Shows information about the filtering server and filtering statistics associated with it.
clear url-server statistics	Clears filtering statistics associated with the filtering server.
filter	Directs traffic to the filtering server. In other words, enables filtering.

url-block	For buffering the Content Server Response
url-server	Identifies a smartfilter (formerly N2H2) or Websense server for use with the filter command.
url-cache	For caching url-server response. This is allowed, only if websense/smartfilter is configured for it.

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(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 FWSM, 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 FWSM 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.

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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 FWSM terminates the connection.

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

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 FWSM before connecting.

username

To add a user to the FWSM local 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* [**encrypted**]} [**privilege** *priv_level*]

no username [*name*]

Syntax Description

encrypted	Indicates that the password is encrypted. When you define a password in the username command, the FWSM 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 keyword. 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 FWSM and you are using the same password.
<i>name</i>	Specifies the name of the user as a string from 4 to 15 characters in length.
nopassword	Indicates that this user needs no password.
password <i>password</i>	Sets the password as a string from 3 to 16 characters in length.
privilege <i>priv_level</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	This command was removed from the system execution space. The system now uses the admin context username database where applicable.

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.

You cannot enter the **username** command in the system execution space. However, when you use the **login** command in system, or use Telnet authentication when you session to the FWSM from the switch, the FWSM uses the admin context username database (Telnet authentication for the system execution space is also configured in the admin context).

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
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 AVPs for specific users.

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 AVPs 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username	•	—	•	—	—

Release	Modification
3.1(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.

The syntax of the commands in attributes 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.

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 FWSM database.

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* [**host** *hostname*] [**warning**]

no virtual http *ip_address* [**host** *hostname*] [**warning**]

Syntax Description

host <i>hostname</i>	(Optional) Assigns a hostname to the virtual HTTP server on the FWSM. When a user is forwarded to the virtual HTTP server to enter their AAA username and password, you see the hostname in the following authentication dialog box message: Username for 'HTTP Authentication (<i>sessionID</i>) from <i>host_name</i> ' at server <i>virtual_http_ip</i> This information helps differentiate the AAA prompt from the destination HTTP server prompt.
<i>ip_address</i>	Sets the IP address for the virtual HTTP server on the FWSM. Make sure this address is an unused address that is routed to the FWSM.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the FWSM. 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	The host keyword was added. Direct authentication with the FWSM was added.

Usage Guidelines

This command enables two functions:

- Cascading HTTP authentications—When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username

and password you used to authenticate with the FWSM 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 FWSM. The FWSM prompts for the AAA server username and password. After the AAA server authenticates the user, the FWSM 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.

**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.

- Direct authentication with the FWSM—You can authenticate directly with the FWSM using the virtual HTTP IP address. 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(S), 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 FWSM, but want to authenticate other types of traffic, you can configure virtual HTTP; the user connects using HTTP to a given IP address configured on the FWSM, and the FWSM provides an HTTP prompt.

You must configure authentication for HTTP access to the virtual HTTP 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 HTTP IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user can successfully access other services that require authentication.

To log out from the FWSM, reconnect to the virtual HTTP IP address; you are prompted to log out.

To use Telnet or SSH instead of HTTP, use the **virtual telnet** or **virtual ssh** command.

Be sure to include the virtual HTTP address as a destination interface in the access list applied to the source interface.

For inbound users (from lower security to higher security), 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, a **static** statement is not required.

Examples

This example shows how to enable virtual HTTP for direct connection along with AAA authentication for other services:

```
hostname(config)# virtual http 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 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 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 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
clear configure virtual	Removes virtual command statements from the configuration.
show running-config virtual	Displays the IP address of the FWSM 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 FWSM to let users authenticate with the FWSM before initiating other types of connections that require authentication.

virtual ssh

To configure a virtual SSH server on the FWSM, use the **virtual ssh** command in global configuration mode. To disable the server, use the **no** form of this command. You might need to authenticate users with the virtual SSH server if you require authentication for types of traffic for which the FWSM does not supply an authentication prompt.

virtual ssh *ip_address*

no virtual ssh *ip_address*

Syntax Description

ip_address Sets the IP address for the virtual SSH server on the FWSM. Make sure this address is an unused address that is routed to the FWSM. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual SSH server, you can use one of the global NAT addresses for the virtual SSH server address.

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
3.2(1)	This command was introduced.

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 FWSM, but want to authenticate other types of traffic, you can configure virtual SSH; the user connects using SSH to a given IP address configured on the FWSM, and the FWSM provides an SSH prompt.

When an unauthenticated user connects to the virtual SSH 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.

To log out from the FWSM, reconnect to the virtual SSH IP address; you are prompted to log out.

To use Telnet or HTTP instead of SSH, use the **virtual telnet** or **virtual http** command.

Examples

The following example shows how to enable virtual SSH along with AAA authentication for other services:

```
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq telnet
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225 eq smtp
hostname(config)# aaa authentication match AUTH inside tacacs+
hostname(config)# virtual ssh 10.1.2.1
```

Related Commands

Command	Description
clear configure virtual	Removes virtual command statements from the configuration.
show running-config virtual	Displays the IP address of the FWSM virtual server.
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
virtual telnet	Allows users to connect to the FWSM using Telnet to perform authentication for the user.

virtual telnet

To configure a virtual Telnet server on the FWSM, 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 FWSM 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 FWSM. Make sure this address is an unused address that is routed to the FWSM.

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
1.1(1)	This command was introduced.

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 FWSM, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the FWSM, and the FWSM 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.

Be sure to include the virtual Telnet address as a destination interface in the access list applied to the source interface.

For inbound users (from lower security to higher security), 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, a **static** statement is not required.

To logout from the FWSM, reconnect to the virtual Telnet IP address; you are prompted to log out.

To use SSH or HTTP instead of Telnet, use the **virtual ssh** or **virtual http** command.

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 FWSM virtual server.
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
virtual ssh	Allows users to connect to the FWSM using SSH to perform authentication for the user.

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.
	<i>time-range</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines

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** form of this command. To remove all configured VPN address assignment methods from the FWSM, use the **no** form of this command without arguments.

vpn-addr-assign {aaa | dhcp | local}

no vpn-addr-assign [aaa | dhcp | local]

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.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

If you choose DHCP, you must also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use.

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.

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 FWSM 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 access list to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the access list, 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 access lists to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those access lists.

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 <i>acl_name</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

WebVPN does not use the access list defined in the **vpn-filter** command.

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.

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for 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
```

Related Commands

Command	Description
vpn-framed-ip-netmask	Provides the subnet mask for this user.

vpn-framed-ip-netmask

To specify the subnet mask to assign to a particular user, use the **vpn-framed-ip-netmask** command in username mode. To remove the subnet mask, use the **no** form of this command.

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

Syntax Description

<i>netmask</i>	Provides the subnet mask for this user.

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
Username attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Examples

The following example shows how to set a subnet mask of 255.255.255. 254 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```

Related Commands

Command	Description
vpn-framed-ip-address	Provides the IP address for this user.

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for 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 FWSM 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 FWSM 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 FWSM 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

<i>minutes</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(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 FWSM terminates the connection.

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** | **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 <i>indexnumber</i>	Logs off a single session by index number. Specify the index number for the session.	
ipaddress <i>IPaddr</i>	Logs off sessions for the IP address that you specify.	
l2l	Logs off all LAN-to-LAN sessions.	
name <i>username</i>	Logs off sessions for the username that you specify.	
protocol <i>protocol-name</i>	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 <i>groupname</i>	Logs off sessions for the tunnel group that you specify.	

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
	3.1(1)	Support for this command was introduced.

Examples

The following example shows how to log off all remote-access sessions:

```
hostname# vpn-sessiondb logoff remote
```

The following 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 FWSM allows, use the **vpn-sessiondb max-session-limit** command in global configuration mode. To remove the session limit, use the **no** form 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

This command applies to all types of VPN sessions, including WebVPN.

Examples

The following example shows how to set a maximum VPN session limit of 450:

```
hostname# vpn-sessiondb max-session-limit 450
```

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 FWSM 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

<i>minutes</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(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 FWSM 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	<i>integer</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines	Enter 0 to disable login and prevent user access.

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), 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

no vpn-tunnel-protocol [IPSec]

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.
webvpn	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

Defaults

IPSec.

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
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

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.

Examples

The following example shows how to configure IPSec tunneling modes for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

who

To display active Telnet administration sessions on the FWSM, 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.

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 FWSM.

Examples

The following example shows the output of the **who** command when a client is logged into the FWSM 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 FWSM console and sets the idle timeout.

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 <i>ip_address</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	—	•

Release	Modification
1.1(1)	This command was introduced.

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
```

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(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 startup configuration for single context mode and for the system in multiple context mode is a hidden file. 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 FWSM 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 FWSM 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

<i>:filename</i>	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 FWSM 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 (:).
<i>server</i> :	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

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 FWSM 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Command History	Release	Modification
	2.2(1)	This command was introduced.

Usage Guidelines 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 FWSM 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 configuration 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.

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	Forces the standby unit to reboot.
reload-standby	

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Privileged EXEC	•	•	•	•	•

Release	Modification
1.1(1)	This command was introduced.

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.

xlate-bypass

To disable NAT sessions for untranslated traffic, use the **xlate-bypass** command in global configuration mode. To disable xlate bypass, use the **no** form of this command.

xlate-bypass

no xlate-bypass

Syntax Description

This command has no arguments or keywords.

Defaults

Xlate bypass 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

By default, the FWSM creates NAT sessions for all connections even if you do not use NAT. For example, a session is created for each untranslated connection even if you do not enable NAT control, you use NAT exemption or identity NAT, or you use same security interfaces and do not configure NAT. Because there is a maximum number of NAT sessions (see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*), these kinds of NAT sessions might cause you to run into the limit.

To avoid running into the limit, you can disable NAT sessions for untranslated traffic using the **xlate-bypass** command. If you disable NAT control and have untranslated traffic or use NAT exemption, or you enable NAT control (using the **nat-control** command) and use NAT exemption, then with xlate bypass, the FWSM does not create a session for these types of untranslated traffic. NAT sessions are still created in the following instances:

- You configure identity NAT (with or without NAT control). Identity NAT is considered to be a translation.
- You use same-security interfaces with NAT control. Traffic between same security interfaces create NAT sessions even when you do not configure NAT for the traffic. To avoid NAT sessions in this case, disable NAT control or use NAT exemption as well as xlate bypass.

Examples

The following example enables xlate bypass:

```
hostname(config)# xlate-bypass
```

Related Commands

Command	Description
nat	Configures NAT.
nat-control	Enables NAT control.
same-security-traffic inter-interface	Allows interfaces on the same security level to communicate.
show running-config xlate-bypass	Shows the xlate bypass configuration.
show xlate	Shows current translation and connection information.

