G through L Commands

gateway

To specify which group of call agents are managing a particular gateway, use the **gateway** command in MGCP map configuration mode. To remove the configuration, use the **no** form of this command.

gateway *ip_address* [*group_id*]

Syntax Description

gateway	Specifies the group of call agents that are managing a particular gateway
ip_address	The IP address of the gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip_address* option. The *group_id* option is a number from 0 to 4294967295 that must correspond with the *group_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

global

To create a pool of mapped addresses for NAT, use the **global** command in global configuration mode. To remove the pool of addresses, use the **no** form of this command.

global (*mapped_ifc) nat_id* {*mapped_ip*[**-***mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[-*mapped_ip*] [**netmask** *mask*] | **interface**}

Syntax Description

interface	Uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP.
mapped_ifc	Specifies the name of the interface connected to the mapped IP address network.
mapped_ip[**-***mapped_ip*]	Specifies the mapped address(es) to which you want to translate the real addresses when they exit the mapped interface. If you specify a single address, then you configure PAT. If you specify a range of addresses, then you configure dynamic NAT. If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC).
nat_id	Specifies an integer for the NAT ID. This ID is referenced by the **nat** command to associate a mapped pool with the real addresses to translate. For regular NAT, this integer is between 1 and 2147483647. For policy NAT (**nat id access-list**), this integer is between 1 and 65535. Do not specify a **global** command for NAT ID 0; 0 is reserved for identity NAT and NAT exemption, which do not use a **global** command.
netmask *mask*	(Optional) Specifies the network mask for the *mapped_ip*. This mask does not specify a network when paired with the *mapped_ip*; rather, it specifies the subnet mask assigned to the *mapped_ip* when it is assigned to a host. If you want to configure a range of addresses, you need to specify *mapped_ip***-***mapped_ip*. If you do not specify a mask, then the default mask for the address class is used.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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 security appliance prevents the user from connecting. If you do not configure group-lock, the security appliance authenticates users without regard to the assigned group.

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

Syntax Description

none	Sets group-lock to a null value, thereby allowing no group-lock restriction. Prevents inheriting a group-lock value from a default or specified group policy.
value *tunnel-grp-name*	Specifies the name of an existing tunnel group that the security appliance requires for the user to connect.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set group lock for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

To add network object groups, use the **group-object** command in protocol, network, service, and icmp-type configuration modes. To remove network object groups, use the **no** form of this command.

group-object *obj_grp_id*

no group-object *obj_grp_id*

Syntax Description

obj_grp_id	Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Protocol, network, service, icmp-type configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **group-object** command is used with the **object-group** command to define an object that itself is an object group. It is used in protocol, network, service, and icmp-type configuration modes. This sub-command allows logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

Duplicate objects are allowed in an object group if they are group objects. For example, if object 1 is in both group A and group B, it is allowed to define a group C which includes both A and B. It is not allowed, however, to include a group object which causes the group hierarchy to become circular. For example, it is not allowed to have group A include group B and then also have group B include group A.

The maximum allowed levels of a hierarchical object group is 10.

Examples

The following example shows how to use the **group-object** command in network configuration mode eliminate the need to duplicate hosts:

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
```

```
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

Syntax Description

external server-group *server_group*	Specifies the group policy as external and identifies the AAA server group for the security appliance to query for attributes.
from *group-policy_name*	Initializes the attributes of this internal group policy to the values of a pre-existing group policy.
internal	Identifies the group policy as internal.
name	Specifies the name of the group policy.
password *server_password*	Provides the password to use when retrieving attributes from the external AAA server group.

Defaults

No default behavior or values. See Usage Guidelines.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

A default group policy, named "DefaultGroupPolicy," always exists on the security appliance. However, this default group policy does not take effect unless you configure the security appliance to use it. For configuration instructions, see the *Cisco Security Appliance Command Line Configuration Guide*.

The DefaultGroupPolicy has these AVPs:

Attribute	Default Value
wins-server	none
dns-server	none
vpn-access-hours	unrestricted

Attribute	Default Value
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 next example shows how to create an external group policy with the name “ExternalGroup,” the AAA server group “BostonAAA,” and the password “12345678”:

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

Related Commands

Command	Description
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.

Command	Description
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, user 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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The 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
clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy	Creates, edits, or removes a group policy.
show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.

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 security appliance without the required license, the security appliance displays an error message.

Syntax Description

map_name	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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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 security appliance ensures secure access over wireless networks, refer to the "Applying Application Layer Protocol Inspection" chapter in the *Cisco Security Appliance Command Line 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 5-1 GTP Map Configuration Commands

Command	Description
description	Specifies the GTP configuration map description.
drop	Specifies the message ID, APN, or GTP version to drop.
help	Displays help for GTP map configuration commands.
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 qtp-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.

help

To display help information for the command specified, use the **help** command in user EXEC mode.

help {*command* | **?**}

Syntax Description

command	Specifies the command for which to display the CLI help.
?	Displays all commands that are available in the current privilege level and mode.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **help** command displays help information about all commands. You can see help for an individual command by entering the **help** command followed by the command name. If you do not specify a command name and enter **?** instead, all commands that are available in the current privilege level and mode display.

If you enable the **pager** command and when 24 lines display, the listing pauses, and the following prompt appears:

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

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

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

Examples

The following example shows how to display help for the **rename** command:

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
```

```
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

The following examples shows how to display help by entering the command name and a question mark:

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

Help is available for the core commands (not the **show**, **no**, or **clear** commands) by entering **?** at the command prompt:

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

homepage

To specify a URL for the web page that displays upon login for this WebVPN user or group policy, use the **homepage** command in webvpn mode, which you enter from group-policy or username mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, use the **homepage none** command.

homepage {value *url-string* **| none}**

no homepage

Syntax Description

none	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting an home page.
value *url-string*	Provides a URL for the home page. The string must begin with either http:// or https://.

Defaults

There is no default home page.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to specify www.example.com as the home page for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.

hostname

To set the security appliance hostname, use the **hostname** command in global configuration mode. To restore the default hostname, use the **no** form of this command. The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

hostname *name*

no hostname [*name*]

Syntax Description

name	Specifies a hostname up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.

Defaults

The default hostname depends on your platform.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	You can no longer use non-alphanumeric characters (other than a hyphen).

Usage Guidelines

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts.

The hostname that you optionally set within a context does not appear in the command line, but can be used for the **banner** command **$(hostname)** token.

Examples

The following example sets the hostname to firewall1:

```
hostname(config)# hostname firewall1
firewall1(config)#
```

Related Commands

Command	Description
banner	Sets a login, message of the day, or enable banner.
domain-name	Sets the default domain name.

html-content-filter

To filter Java, ActiveX, images, scripts, and cookies for WebVPN sessions for this user or group policy, use the **html-content-filter** command in webvpn mode, which you enter from group-policy or username mode. To remove a content filter, use the **no** form of this command. To remove all content filters, including a null value created by issuing the **html-content-filter none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an html content filter, use the **html-content-filter none** command.

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

Syntax Description

cookies	Removes cookies from images, providing limited ad filtering and privacy.
images	Removes references to images (removes <IMG> tags).
java	Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags.
none	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
scripts	Removes references to scripting (removes <SCRIPT> tags).

Defaults

No filtering occurs.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Using the command a second time overrides the previous setting.

Examples

The following example shows how to set filtering of JAVA and ActiveX, cookies, and images for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

Related Commands

Command	Description
webvpn (group-policy, username)	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

http

To specify hosts that can access the HTTP server internal to the security appliance, use the **http** command in global configuration mode. To remove one or more hosts, use the **no** form of this command. To remove the attribute from the configuration, use the **no** form of this command without arguments.

http *ip_address subnet_mask interface_name*

no http

Syntax Description

interface_name	Provides the name of the security appliance interface through which the host can access the HTTP server.
ip_address	Provides the IP address of a host that can access the HTTP server.
subnet_mask	Provides the subnet mask of a host that can access the HTTP server.

Defaults

No hosts can access the HTTP server.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to allow the host with the IP address of 10.10.99.1 and the subnet mask of 255.255.255.255 access to the HTTP server via the outside interface:

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

The next example shows how to allow any host access to the HTTP server via the outside interface:

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.

Command	Description
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http 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 security appliance validates certificates against the PKI trust points. If a certificate does not pass validation, the security appliance closes the SSL connection.

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

Syntax Description

interface	Specifies the interface on the security appliance 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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You 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 security appliance interface through which the host accesses the HTTP server.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http redirect

To specify that the security appliance redirect HTTP connections to HTTPS, use the **http redirect** command in global configuration mode. To remove a specified http redirect command from the configuration, use the **no** version of this command. To remove all http redirect commands from the configuration, use the **no** version of this command without arguments.

http redirect *interface* [*port*]

no http redirect [*interface*]

Syntax Description

interface	Identifies the interface for which the security appliance should redirect HTTP requests to HTTPS.
port	Identifies the port the security appliance listens on for HTTP requests, which it then redirects to HTTPS. By default it listens on port 80,

Defaults

HTTP redirect is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The interface requires an access list that permits HTTP. Otherwise the security appliance does not listen to port 80, or to any other port that you configure for HTTP.

Examples

The following example shows how to configure HTTP redirect for the inside interface, keeping the default port 80:

```
hostname(config)# http redirect inside
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http server enable	Enables the HTTP server.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

http server enable

To enable the security appliance HTTP server, use the **http server enable** command in global configuration mode. To disable the HTTP server, use the **no** form of this command.

http server enable

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to enable the HTTP server.

```
hostname(config)# http server enable
```

Related Commands

Command	Description
clear configure http	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
show running-config http	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

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:

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

Command History

Release	Modification
7.0	This command was introduced in 7.0.

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 security appliance 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 5-2 summarizes the configuration commands available in HTTP map configuration mode. Click on an entry to open a command page that provides the detailed syntax for each command.

Table 5-2 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 security appliance to reset the connection and create a syslog entry when it detects any traffic that contain the following:

- Messages less than 100 bytes or exceeding 2000 bytes
- Unsupported content types
- HTTP headers exceeding 100 bytes

- URIs exceeding 100 bytes

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

http-proxy

To configure an HTTP proxy server, use the **http-proxy** command in webvpn mode. To remove the HTTP proxy server from the configuration, use the **no** form of this command.

This is an external proxy server the security appliance uses for HTTP requests.

http-proxy *address* [*port*]

no http-proxy

Syntax Description

address	Specifies the IP address for the external HTTP proxy server.
port	Specifies the port the HTTP proxy server uses. The default port is 80, which is the port the security appliance uses if you do not supply a value.

Defaults

No HTTP proxy server is configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to configure an HTTP proxy server with an IP address of 10.10.10.7 using port 80:

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 10.10.10.7
```

https-proxy

To configure an HTTPS proxy server, use the **https-proxy** command in webvpn mode. To remove the HTTPS proxy server from the configuration, use the no form of this command.

This is an external proxy server the security appliance uses for HTTPS requests.

https-proxy *address* [*port*]

no https-proxy

Syntax Description

address	Specifies the IP address for the external HTTPS proxy server.
port	Specifies the port the HTTPS proxy server uses. The default port is 443, which is the port the security appliance uses if you do not supply a value.

Defaults

No HTTPS proxy server is configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to configure an HTTPS proxy server with an IP address of 10.10.10.1 using port 443:

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 10.10.10.1 443
```

hw-module module recover

To load a recovery software image from a TFTP server to an intelligent SSM (for example, the AIP SSM), or to configure network settings to access the TFTP server, use the **hw-module module recover** command in privileged EXEC mode. You might need to recover an SSM using this command if, for example, the SSM is unable to load a local image. This command is not available for interface SSMs (for example, the 4GE SSM).

hw-module module 1 recover {**boot** | **stop** | **configure** [**url** *tfp_url* | **ip** *port_ip_address* | **gateway** *gateway_ip_address* | **vlan** *vlan_id*]}

Syntax Description

1	Specifies the slot number, which is always 1.
boot	Initiates recovery of this SSM and downloads a recovery image according to the **configure** settings. The SSM then reboots from the new image.
configure	Configures the network parameters to download a recovery image. If you do not enter any network parameters after the **configure** keyword, you are prompted for the information.
gateway *gateway_ip_address*	(Optional) The gateway IP address for access to the TFTP server through the SSM management interface.
ip *port_ip_address*	(Optional) The IP address of the SSM management interface.
stop	Stops the recovery action, and stops downloading the recovery image. The SSM boots from the original image. You must enter this command within 30 to 45 seconds after starting recovery using the **hw-module module boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the SSM becoming unresponsive.
url *tfp_url*	(Optional) The URL for the image on a TFTP server, in the following format: **tftp://***server*/[*path*/]*filename*
vlan *vlan_id*	(Optional) Sets the VLAN ID for the management interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is only available when the SSM is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information.

Examples

The following example sets the SSM to download an image from a TFTP server:

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

The following example recovers the SSM:

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module reload

To reload an intelligent SSM software (for example, the AIP SSM), use the **hw-module module reload** command in privileged EXEC mode. This command is not available for interface SSMs (for example, the 4GE SSM).

hw-module module 1 reload

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is only valid when the SSM status is Up. See the **show module** command for state information.

This command differs from the **hw-module module reset** command, which also performs a hardware reset.

Examples

The following example reloads the SSM in slot 1:

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

Command	Description
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module reset

To shut down and reset the SSM hardware, use the **hw-module module reset** command in privileged EXEC mode.

hw-module module 1 reset

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is only valid when the SSM status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

When the SSM is in an Up state, the **hw-module module reset** command prompts you to shut down the software before resetting.

You can recover intelligent SSMs (for example, the AIP SSM) using the **hw-module module recover** command. If you enter the **hw-module module reset** while the SSM is in a Recover state, the SSM does not interrupt the recovery process. The the **hw-module module reset** command performs a hardware reset of the SSM, and the SSM recovery continues after the hardware reset. You might want to reset the SSM during recovery if the SSM hangs; a hardware reset might resolve the issue.

This command differs from the **hw-module module reload** command which only reloads the software and does not perform a hardware reset.

Examples

The following example resets an SSM in slot 1 that is in the Up state:

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

```
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.
show module	Shows SSM information.

hw-module module shutdown

To shut down the SSM software, use the **hw-module module shutdown** command in privileged EXEC mode.

hw-module module 1 shutdown

Syntax Description

1	Specifies the slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Shutting down the SSM software prepares the SSM to be safely powered off without losing configuration data.

This command is only valid when the SSM status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down an SSM in slot 1:

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

Command	Description
hw-module module reload	Reloads the intelligent SSM software.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
show module	Shows SSM information.

icmp

To configure access rules for ICMP traffic that terminates at a security appliance interface, use the **icmp** command. To remove the configuration, use the **no** form of this command.

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

Syntax Description

deny	Deny access if the conditions are matched.
icmp_type	(Optional) ICMP message type (see Table 5-3).
if_name	The interface name.
ip_address	The IP address of the host sending ICMP messages to the interface.
net_mask	The mask to be applied to *ip_address*.
permit	Permit access if the conditions are matched.

Defaults

The default behavior of the security appliance is to allow all ICMP traffic *to* the security appliance interfaces. However, by default the security appliance does not respond to ICMP echo requests directed to a broadcast address. The security appliance also denies ICMP messages received at the outside interface for destinations on a protected interface.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was previously existing.

Usage Guidelines

The **icmp** command controls ICMP traffic that terminates on any security appliance interface. If no ICMP control list is configured, then the security appliance accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the security appliance does not respond to ICMP echo requests directed to a broadcast address.

The security appliance only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

The **icmp deny** command disables pinging to an interface, and the **icmp permit** command enables pinging to an interface. With pinging disabled, the security appliance cannot be detected on the network. This is also referred to as configurable proxy pinging.

Use the **access-list extended** or **access-group** commands for ICMP traffic that is routed *through* the security appliance for destinations on a protected interface.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP Path MTU discovery, which can halt IPSec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If an ICMP control list is configured for an interface, then the security appliance first matches the specified ICMP traffic and then applies an implicit deny for all other ICMP traffic on that interface. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a **permit** statement is assumed.

Table 5-3 lists the supported ICMP type values.

Table 5-3 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
```

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **icmp-object** command is used with the **object-group** command to define an icmp-type object. It is used in icmp-type configuration mode.

ICMP type numbers and names include:

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**

Number	ICMP Type Name
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

Examples

The following example shows how to use the **icmp-object** command in icmp-type configuration mode:

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

id-cert-issuer

To indicate whether the system accepts peer certificates issued by the CA associated with this trustpoint, use the **id-cert-issuer** command in crypto ca trustpoint configuration mode. Use the **no** form of this command to disallow certificates that were issued by the CA associated with the trustpoint. This is useful for trustpoints that represent widely used root CAs.

id-cert-issuer

no id-cert-issuer

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is enabled (identity certificates are accepted).

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use this command to limit certificate acceptance to those issued by the subordinate certificate of a widely used root certificate. If you do not allow this feature, the security appliance rejects any IKE peer certificate signed by this issuer.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and lets an administrator accept identity certificates signed by the issuer for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint submode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

igmp

To reinstate IGMP processing on an interface, use the **igmp** command in interface configuration mode. To disable IGMP processing on an interface, use the **no** form of this command.

igmp

no igmp

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Only the **no** form of this command appears in the running configuration.

Examples

The following example disables IGMP processing on the selected interface:

```
hostname(config-if)# no igmp
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.
show igmp interface	Displays multicast information for an interface.

igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **igmp access-group** command in interface configuration mode. To disable groups on the interface, use the **no** form of this command.

igmp access-group *acl*

no igmp access-group *acl*

Syntax Description

acl	Name of an IP access list. You can specify a standard or and extended access list. However, if you specify an extended access list, only the destination address is matched; you should specify **any** for the source.

Defaults

All groups are allowed to join on an interface.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Examples

The following example limits hosts permitted by access list 1 to join the group:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp forward interface

To enable forwarding of all IGMP host reports and leave messages received to the interface specified, use the **igmp forward interface** command in interface configuration mode. To remove the forwarding, use the **no** form of this command.

igmp forward interface *if-name*

no igmp forward interface *if-name*

Syntax Description

if-name	Logical name of the interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Enter this command on the input interface. This command is used for stub multicast routing and cannot be configured concurrently with PIM.

Examples

The following example forwards IGMP host reports from the current interface to the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

igmp join-group

To configure an interface to be a locally connected member of the specified group, use the **igmp join-group** command in interface configuration mode. To cancel membership in the group, use the **no** form of this command.

igmp join-group *group-address*

no igmp join-group *group-address*

Syntax Description

group-address	IP address of the multicast group.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command configures a security appliance interface to be a member of a multicast group. The **igmp join-group** command causes the security appliance to both accept and forward multicast packets destined for the specified multicast group.

To configure the security appliance to forward the multicast traffic without being a member of the multicast group, use the **igmp static-group** command.

Examples

The following example configures the selected interface to join the IGMP group 255.2.2.2:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

Related Commands

Command	Description
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp limit

To limit the number of IGMP states on a per-interface basis, use the **igmp limit** command in interface configuration mode. To restore the default limit, use the **no** form of this command.

igmp limit *number*

no igmp limit [*number*]

Syntax Description

number	Number of IGMP states allowed on the interface. Valid values range from 0 to 500. The default value is 500. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the **igmp join-group** and **igmp static-group** commands) are still permitted.

Defaults

The default is 500.

Command Modes

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

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

Command History

Release	Modification
7.0	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 gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

Related Commands

Command	Description
igmp	Reinstates IGMP processing on an interface.
igmp join-group	Configure an interface to be a locally connected member of the specified group.
igmp static-group	Configure the interface to be a statically connected member of the specified multicast group.

igmp query-interval

To configure the frequency at which IGMP host query messages are sent by the interface, use the **igmp query-interval** command in interface configuration mode. To restore the default frequency, use the **no** form of this command.

igmp query-interval *seconds*

no igmp query-interval *seconds*

Syntax Description

seconds	Frequency, in seconds, at which to send IGMP host query messages. Valid values range from 1 to 3600. The default is 125 seconds.

Defaults

The default query interval is 125 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

Multicast routers send host query messages to discover which multicast groups have members on the networks attached to the interface. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Host query messages are addressed to the all-hosts multicast group, which has an address of 224.0.0.1 TTL value of 1.

The designated router for a LAN is the only router that sends IGMP host query messages:

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Version 2, the designated router is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the **igmp query-timeout** command), it becomes the querier.

Caution Changing this value may severely impact multicast forwarding.

Examples

The following example changes the IGMP query interval to 120 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-max-response-time

To specify the maximum response time advertised in IGMP queries, use the **igmp query-max-response-time** command in interface configuration mode. To restore the default response time value, use the **no** form of this command.

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. Valid values are from 1 to 25. The default value is 10 seconds.

Defaults

10 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

This command is valid only when IGMP Version 2 or 3 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example changes the maximum query response time to 8 seconds:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

igmp query-timeout

To configure the timeout period before the interface takes over as the querier after the previous querier has stopped querying, use the **igmp query-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. Valid values are from 60 to 300 seconds. The default value is 255 seconds.

Defaults

The default query interval is 255 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command requires IGMP Version 2 or 3.

Examples

The following example configures the router to wait 200 seconds from the time it received the last query before it takes over as the querier for the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

Related Commands

Command	Description
igmp query-interval	Configures the frequency at which IGMP host query messages are sent by the interface.
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.

igmp static-group

To configure the interface to be a statically connected member of the specified multicast group, use the **igmp static-group** command in interface configuration mode. To remove the static group entry, use the **no** form of this command.

igmp static-group *group*

no igmp static-group *group*

Syntax Description

group	IP multicast group address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When configured with the **igmp static-group** command, the security appliance interface does not accept multicast packets destined for the specified group itself; it only forwards them. To configure the security appliance both accept and forward multicast packets for a speific multicast group, use the **igmp join-group** command. If the **igmp join-group** command is configured for the same group address as the **igmp static-group** command, the **igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Examples

The following example adds the selected interface to the multicast group 239.100.100.101:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

Related Commands

Command	Description
igmp join-group	Configures an interface to be a locally connected member of the specified group.

igmp version

To configure which version of IGMP the interface uses, use the **igmp version** command in interface configuration mode. To restore version to the default, use the **no** form of this command.

igmp version {**1** | **2**}

no igmp version [**1** | **2**]

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.

Defaults

IGMP Version 2.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was moved to interface configuration mode. Earlier versions required you to enter multicast interface configuration mode, which is no longer available.

Usage Guidelines

All routers on the subnet must support the same version of IGMP. Hosts can have any IGMP version (1 or 2) and the security appliance will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2, such as the **igmp query-max-response-time** and **igmp query-timeout** commands.

Examples

The following example configures the selected interface to use IGMP Version 1:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

Related Commands

Command	Description
igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
igmp query-timeout	Configures the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

ignore 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Type 6 MOSPF packets are unsupported.

Examples

The following example cause LSA Type 6 MOSPF packets to be ignored:

```
hostname(config-router)# ignore lsa mospf
```

Related Commands

Command	Description
show running-config router ospf	Displays the OSPF router configuration.

imap4s

To enter IMAP4S configuration mode, use the **imap4s** command in global configuration mode. To remove any commands entered in IMAP4S command mode, use the **no** form of this command.

IMAP4 is a client/server protocol in which your Internet server receives and holds e-mail for you. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate multiple folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail. IMAP4S lets you receive e-mail over an SSL connection.

imap4s

no imap4s

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to enter IMAP4S configuration mode:

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
show running-config imap4s	Displays the running configuration for IMAP4S.

inspect ctiqbe

To enable CTIQBE protocol inspection, use the **inspect ctiqbe** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To disable inspection, use the **no** form of this command.

inspect ctiqbe

no inspect ctiqbe

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced in 7.0. It replaces the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect ctiqbe** command enables CTIQBE protocol inspection, which supports NAT, PAT, and bidirectional NAT. This enables Cisco IP SoftPhone and other Cisco TAPI/JTAPI applications to work successfully with Cisco CallManager for call setup across the security appliance.

The Telephony Application Programming Interface (TAPI) and Java Telephony Application Programming Interface (JTAPI) are used by many Cisco VoIP applications. Computer Telephony Interface Quick Buffer Encoding (CTIQBE) is used by Cisco TAPI Service Provider (TSP) to communicate with Cisco CallManager.

The following summarizes limitations that apply when using CTIQBE application inspection:

- CTIQBE application inspection does not support configurations using the **alias** command.
- Stateful Failover of CTIQBE calls is *not* supported.
- Using the **debug ctiqbe** command may delay message transmission, which may have a performance impact in a real-time environment. When you enable this debugging or logging and Cisco IP SoftPhone seems unable to complete call setup through the security appliance, increase the timeout values in the Cisco TSP settings on the system running Cisco IP SoftPhone.
- CTIQBE application inspection does *not* support CTIQBE messages fragmented in multiple TCP packets.

The following summarizes special considerations when using CTIQBE application inspection in specific scenarios:

- If two Cisco IP SoftPhones are registered with different Cisco CallManagers, which are connected to different interfaces of the security appliance, calls between these two phones will fail.
- When Cisco CallManager is located on the higher security interface compared to Cisco IP SoftPhones, if NAT or outside NAT is required for the Cisco CallManager IP address, the mapping must be static as Cisco IP SoftPhone requires the Cisco CallManager IP address to be specified explicitly in its Cisco TSP configuration on the PC.
- When using PAT or Outside PAT, if the Cisco CallManager IP address is to be translated, its TCP port 2748 must be statically mapped to the **same port** of the PAT (interface) address for Cisco IP SoftPhone registrations to succeed. The CTIQBE listening port (TCP 2748) is fixed and is not user-configurable on Cisco CallManager, Cisco IP SoftPhone, or Cisco TSP.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect ctiqbe** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect ctiqbe** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect ctiqbe** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the CTIQBE inspection engine as shown in the following example, which creates a class map to match CTIQBE traffic on the default port (2748). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

To enable CTIQBE inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show conn	Displays the connection state for different connection types.
show ctiqbe	Displays information regarding the CTIQBE sessions established across the security appliance. Displays information about the media connections allocated by the CTIQBE inspection engine.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect cuseeme

To enable CU-SeeMe application inspection or to change the ports to which the security appliance listens, use the **inspect cuseeme 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 cuseeme

no inspect cuseeme

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect cuseeme** command provides application inspection for the CU-SeeMe application.

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.

With CU-SeeMe clients, one user can connect directly to another (CU-SeeMe or other H.323 client) for person-to-person audio, video, and data collaboration. CU-SeeMe clients can conference in a mixed client environment that includes both CU-SeeMe clients and H.323-compliant clients from other vendors.

In the background, CU-SeeMe clients operate in two very different modes. When connected to another CU-SeeMe client or CU-SeeMe Conference Server, the client sends information in CU-SeeMe mode.

When connected to an H.323-compliant videoconferencing client from a different vendor, CU-SeeMe clients communicate using the H.323-standard format in H.323 mode.

CU-SeeMe is supported through H.323 inspection, as well as performing NAT on the CU-SeeMe control stream, which operates on UDP port 7648.

Examples

You enable the CU-SeeMe inspection engine as shown in the following example, which creates a class map to match CU-SeeMe traffic on the default port (7648). The service policy is then applied to the outside interface.

```
hostname(config)# class-map cuseeme-port
hostname(config-cmap)# match port tcp eq 7648
hostname(config-cmap)# exit
hostname(config)# policy-map cuseeme_policy
hostname(config-pmap)# class cuseeme-port
hostname(config-pmap-c)# inspect cuseeme
hostname(config-pmap-c)# exit
hostname(config)# service-policy cuseeme_policy interface outside
```

To enable CU-SeeMe 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 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
max_pkt_length	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:

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** 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 security appliance. DNS guard also monitors the message exchange to ensure that the ID of the DNS reply matches the ID of the DNS query.

When DNS inspection is enabled, which it is the default, the security appliance performs the following additional tasks:

- Translates the DNS record based on the configuration completed using the **alias**, **static** and **nat** commands (DNS rewrite). Translation only applies to the A-record in the DNS reply. Therefore, reverse lookups, which request the PTR record, are not affected by DNS rewrite.

Note DNS rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.

- Enforces the maximum DNS message length (the default is 512 bytes and the maximum length is 65535 bytes). Reassembly is performed as necessary to verify that the packet length is less than the maximum length configured. The packet is dropped if it exceeds the maximum length.

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 security appliance within a limited period of time and there is no resource build-up. However, if you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

How DNS Rewrite Works

When DNS inspection is enabled, DNS rewrite provides full support for NAT of DNS messages originating from any interface.

If a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS A-record is translated correctly. If the DNS inspection engine is disabled, the A-record is not translated.

DNS rewrite performs two functions:

- Translating a public address (the routable or “mapped” address) in a DNS reply to a private address (the “real” address) when the DNS client is on a private interface.
- Translating a private address to a public address when the DNS client is on the public interface.

As long as DNS inspection remains enabled, you can configure DNS rewrite using the **alias**, **static**, or **nat** commands. For details about the syntax and function of these commands, refer to the appropriate command page.

Examples

The following example 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
dns-guard	Enables the DNS guard function.
class-map	Defines the traffic class to which to apply security actions.
debug dns	Enables debug information for DNS.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect esmtp

To enable SMTP application inspection or to change the ports to which the security appliance listens, use the **inspect esmtp** command in class configuration mode. The class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect esmtp

no inspect esmtp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

ESMTP application inspection provides improved protection against SMTP-based attacks by restricting the types of SMTP commands that can pass through the security appliance and by adding monitoring capabilities.

ESMTP is an enhancement to the SMTP protocol and is similar is most respects to SMTP. For convenience, the term SMTP is used in this document to refer to both SMTP and ESMTP. The application inspection process for extended SMTP is similar to SMTP application inspection and includes support for SMTP sessions. Most commands used in an extended SMTP session are the same as those used in an SMTP session but an ESMTP session is considerably faster and offers more options related to reliability and security, such as delivery status notification.

The **inspect esmtp** command includes the functionality previously provided by the **fixup smtp** command, and provides additional support for some extended SMTP commands. Extended SMTP application inspection adds support for eight extended SMTP commands, including AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML and VRFY. Along with the support for seven RFC 821 commands (DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET), the security appliance supports a total of fifteen SMTP commands.

Other extended SMTP commands, such as ATRN, STARTLS, ONEX, VERB, CHUNKING, and private extensions and are not supported. Unsupported commands are translated into Xs, which are rejected by the internal server. This results in a message such as "500 Command unknown: 'XXX'." Incomplete commands are discarded.

If you enter the **inspect smtp** command, the security appliance automatically converts the command into **inspect esmtp**, which is the configuration that will be shown if you enter the **show running-config** command.

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 security appliance changes all the characters in the packet to X. In this case, the server will generate an error code to the client. Because of the change in the packet, the TCP checksum has to be recalculated or adjusted.
- TCP stream editing.
- Command pipelining.

Examples

You enable the SMTP inspection engine as shown in the following example, which creates a class map to match SMTP traffic on the default port (25). The service policy is then applied to the outside interface.

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

To enable SMTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug smtp	Enables debug information for SMTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SMTP.

inspect ftp

To configure the port for FTP inspection or to enable enhanced inspection, use the **inspect ftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

Syntax Description

map_name	The name of the FTP map.
strict	(Optional) Enables enhanced inspection of FTP traffic and forces compliance with RFC standards.

Caution Use caution when moving FTP to a higher port. For example, if you set the FTP port to 2021, all connections that initiate to port 2021 will have their data payload interpreted as FTP commands.

Defaults

The security appliance listens to port 21 for FTP by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated. The *map_name* option was added.

Usage Guidelines

The FTP application inspection inspects the FTP sessions and performs four tasks:

- Prepares dynamic secondary data connections
- Tracks **ftp** command-response sequence
- Generates an audit trail
- NATs embedded IP addresses

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 security appliance replaces the FTP server response to the SYST command with a series of Xs. to prevent the server from revealing its system type to FTP clients. To override this default behavior, use the **no mask-syst-reply** command in FTP map configuration mode.

Note To identify specific FTP commands that are not permitted to pass through the security appliance, identify an FTP map and use the **request-command deny** command. For details, see the **ftp-map** and the **request-command deny** command pages.

FTP Log Messages

FTP application inspection generates the following log messages:

- An Audit record 302002 is generated for each file that is retrieved or uploaded.

- The **ftp** command is checked to see if it is RETR or STOR and the retrieve and store commands are logged.
- The username is obtained by looking up a table providing the IP address.
- The username, source IP address, destination IP address, NAT address, and the file operation are logged.
- Audit record 201005 is generated if the secondary dynamic channel preparation failed due to memory shortage.

In conjunction with NAT, the FTP application inspection translates the IP address within the application payload. This is described in detail in RFC 959.

Examples

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 security appliance 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 security appliance without the required license, the security appliance displays an error message.

Syntax Description

map_name	(Optional) Name for the GTP map.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

GTP is the tunnelling protocol for GPRS, and helps provide secure access over wireless networks. GPRS is a data network architecture that is designed to integrate with existing GSM networks. It offers mobile subscribers uninterrupted, packet-switched data services to corporate networks and the Internet. For an overview of GTP, refer to the "Applying Application Layer Protocol Inspection" chapter in the *Cisco Security Appliance Command Line 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, us other static routing or dynamic routing.

Examples

The following example shows how to use access lists to identify GTP traffic, define a GTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

Note This example enables GTP inspection with the default values. To change the default values, refer to the **gtp-map** command page and to the command pages for each command that is entered from GTP map configuration mode.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
service-policy	Applies a policy map to one or more interfaces.

inspect h323

To enable H.323 application inspection or to change the ports to which the security appliance listens, use the **inspect h323** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect h323 {**h225** | **ras** }

no inspect h323 {**h225** | **ras** }

Syntax Description

h225	Enables H.225 signalling inspection.
ras	Enables RAS inspection.

Defaults

The default port assignments are as follows:

- h323 h225 1720
- h323 ras 1718-1719

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect h323** command provides support for H.323 compliant applications such as Cisco CallManager and VocalTec Gatekeeper. H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. The security appliance supports H.323 through Version 4, including the H.323 v3 feature Multiple Calls on One Call Signaling Channel.

With H.323 inspection enabled, the security appliance supports multiple calls on the same call signaling channel, a feature introduced with H.323 Version 3. This feature reduces call setup time and reduces the use of ports on the security appliance.

The two major functions of H.323 inspection are as follows:

- NAT the necessary embedded IPv4 addresses in the H.225 and H.245 messages. Because H.323 messages are encoded in PER encoding format, the security appliance uses an ASN.1 decoder to decode the H.323 messages.

- Dynamically allocate the negotiated H.245 and RTP/RTCP connections.

How H.323 Works

The H.323 collection of protocols collectively may use up to two TCP connection and four to six UDP connections. FastStart uses only one TCP connection, and RAS uses a single UDP connection for registration, admissions, and status.

An H.323 client may initially establish a TCP connection to an H.323 server using TCP port 1720 to request Q.931 call setup. As part of the call setup process, the H.323 terminal supplies a port number to the client to use for an H.245 TCP connection. The H.245 connection is for call negotiation and media channel setup. In environments where H.323 gatekeeper is in use, the initial packet is transmitted using UDP.

H.323 inspection monitors the Q.931 TCP connection to determine the H.245 port number. If the H.323 terminals are not using FastStart, the security appliance dynamically allocates the H.245 connection based on the inspection of the H.225 messages.

Note The H.225 connection can also be dynamically allocated when using RAS.

Within each H.245 message, the H.323 endpoints exchange port numbers that are used for subsequent UDP data streams. H.323 inspection inspects the H.245 messages to identify these ports and dynamically creates connections for the media exchange. Real-Time Transport Protocol (RTP) uses the negotiated port number, while RTP Control Protocol (RTCP) uses the next higher port number.

The H.323 control channel handles H.225 and H.245 and H.323 RAS. H.323 inspection uses the following ports.

- 1718—UDP port used for gatekeeper discovery
- 1719—UDP port used for RAS and for gatekeeper discovery
- 1720—TCP Control Port

If the ACF message from the gatekeeper goes through the security appliance, a pinhole will be opened for the H.225 connection. The H.245 signaling ports are negotiated between the endpoints in the H.225 signaling. When an H.323 gatekeeper is used, the security appliance opens an H.225 connection based on inspection of the ACF message. If | the security appliance does not see the ACF message, you might need to open an access list for the well-known H.323 port 1720 for the H.225 call signaling.

The security appliance dynamically allocates the H.245 channel after inspecting the H.225 messages and then hooks up to the H.245 channel to be fixed up as well. That means whatever H.245 messages pass through the security appliance pass through the H.245 application inspection, NATing embedded IP addresses and opening the negotiated media channels.

The H.323 ITU standard requires that a TPKT header, defining the length of the message, precede the H.225 and H.245, before being passed on to the reliable connection. Because the TPKT header does not necessarily need to be sent in the same TCP packet as the H.225/H.245 message, the security appliance must remember the TPKT length to process/decode the messages properly. The security appliance keeps a data structure for each connection and that data structure contains the TPKT length for the next expected message.

If the security appliance needs to NAT any IP addresses, then it will have to change the checksum, the UUIE (user-user information element) length, and the TPKT, if included in the TCP packet with the H.225 message. If the TPKT is sent in a separate TCP packet, then the security appliance will proxy ACK that TPKT and append a new TPKT to the H.245 message with the new length.

Note The security appliance does not support TCP options in the Proxy ACK for the TPKT.

Each UDP connection with a packet going through H.323 inspection is marked as an H.323 connection and will time out with the H.323 timeout as configured using the **timeout** command.

Limitations and Restrictions

The following are some of the known issues and limitations when using H.323 application inspection:

- Static PAT may not properly translate IP addresses embedded in optional fields within H.323 messages. If you experience this kind of problem, do not use static PAT with H.323.
- It has been observed that when a NetMeeting client registers with an H.323 gatekeeper and tries to call an H.323 gateway that is also registered with the H.323 gatekeeper, the connection is established but no voice is heard in either direction. This problem is unrelated to the security appliance.
- If you configure a network static where the network static is the same as a third-party netmask and address, then any outbound H.323 connection fails.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect h323** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect h323** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect h323** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the H.323 inspection engine as shown in the following example, which creates a class map to match H.323 traffic on the default port (1720). The service policy is then applied to the outside interface.

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

To enable H.323 inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
show h225	Displays information for H.225 sessions established across the security appliance.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.

Commands	Description
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout {**h225** | **h323**}	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

inspect http

To enable HTTP application inspection or to change the ports to which the security appliance listens, use the **inspect http command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect http [*map_name*]

no inspect http [*map_name*]

Syntax Description

map_name	(Optional) The name of the HTTP map.

Defaults

The default port for HTTP is 80.

Enhanced HTTP inspection is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect http** command protects against specific attacks and other threats that may be associated with HTTP traffic. HTTP inspection performs several functions:

- Enhanced HTTP inspection
- URL screening through N2H2 or Websense
- Java and ActiveX filtering

The latter two features are configured in conjunction with the **filter** command.

Enhanced HTTP inspection verifies that HTTP messages conform to RFC 2616, use RFC-defined methods or supported extension methods, and comply with various other criteria. In many cases, you can configure these criteria and the system response when the criteria are not met. The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

The criteria that you can apply to HTTP messages include the following:

- Does not include any method on a configurable list.

- Specific transfer encoding method or application type.
- HTTP transaction adheres to RFC specification.
- Message body size is within configurable limits.
- Request and response message header size is within a configurable limit.
- URI length is within a configurable limit.
- The content-type in the message body matches the header.
- The content-type in the response message matches the *accept-type* field in the request message.
- The content-type in the message is included in a predefined internal list.
- Message meets HTTP RFC format criteria.
- Presence or absence of selected supported applications.
- Presence or absence of selected encoding types.

Note The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

To enable enhanced HTTP inspection, enter the **inspect http** *http-map* command. The rules that this applies to HTTP traffic are defined by the specific HTTP map, which you configure by entering the **http-map** command and HTTP map configuration mode commands.

Note When you enable HTTP inspection with an HTTP map, strict HTTP inspection with the action reset and log is enabled by default. You can change the actions performed in response to inspection failure, but you cannot disable strict inspection as long as the HTTP map remains enabled.

Examples

The following example shows how to identify HTTP traffic, define an HTTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

This example causes the security appliance to reset the connection and create a syslog entry when it detects any traffic that contain the following:

- Messages less than 100 bytes or exceeding 2000 bytes

- Unsupported content types
- HTTP headers exceeding 100 bytes
- URIs exceeding 100 bytes

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about HTTP application inspection.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
policy-map	Associates a class map with specific security actions.

inspect icmp

To configure the ICMP inspection engine, use the **inspect icmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode.

inspect icmp

no inspect icmp

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The ICMP inspection engine allows ICMP traffic to be inspected like TCP and UDP traffic. Without the ICMP inspection engine, we recommend that you do not allow ICMP through the security appliance in an ACL. Without stateful inspection, ICMP can be used to attack your network. The ICMP inspection engine ensures that there is only one response for each request, and that the sequence number is correct

When ICMP inspection is disabled, which is the default configuration, ICMP echo reply messages are denied from a lower security interface to a higher security interface, even if it is in response to an ICMP echo request.

Examples

You enable the ICMP application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

To enable ICMP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect icmp error

To enable application inspection for ICMP error messages, use the **inspect icmp error** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode.

inspect icmp error

no inspect icmp error

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

Use the **inspect icmp error** command to create xlates for intermediate hops that send ICMP error messages, based on the static/NAT configuration. By default, the security appliance hides the IP addresses of intermediate hops. However, using the **inspect icmp error** command makes the intermediate hop IP addresses visible. The security appliance overwrites the packet with the translated IP addresses.

When enabled, the ICMP error inspection engine makes the following changes to the ICMP packet:

- In the IP Header, the NAT IP is changed to the Client IP (Destination Address and Intermediate Hop Address) and the IP checksum is modified.
- In the ICMP Header, the ICMP checksum is modified due to the changes in the ICMP packet.
- In the Payload, the following changes are made:
  - Original packet NAT IP is changed to the Client IP
  - Original packet NAT port is changed to the Client Port
  - Original packet IP checksum is recalculated

When an ICMP error message is retrieved, whether ICMP error inspection is enabled or not, the ICMP payload is scanned to retrieve the five-tuple (src ip , dest ip, src port, dest port, and ip protocol) from the original packet. A lookup is performed, using the retrieved five-tuple, to determine the original address of the client and to locate an existing session associated with the specific five-tuple. If the session is not found, the ICMP error message is dropped.

Examples

You enable the ICMP error application inspection engine as shown in the following example, which creates a class map to match ICMP traffic using the ICMP protocol ID, which is 1 for IPv4 and 58 for IPv6. The service policy is then applied to the outside interface.

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

To enable ICMP error inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
inspect icmp	Enables or disables the ICMP inspection engine.
policy-map	Defines a policy that associates security actions with one or more traffic classes.
service-policy	Applies a policy map to one or more interfaces.

inspect ils

To enable ILS application inspection or to change the ports to which the security appliance 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:

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect ils** command provides NAT support for Microsoft NetMeeting, SiteServer, and Active Directory products that use LDAP to exchange directory information with an ILS server.

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 security appliance supports NAT for ILS, which is used to register and locate endpoints in the ILS or SiteServer Directory. PAT cannot be supported because only IP addresses are stored by an LDAP database.

For search responses, when the LDAP server is located outside, NAT should be considered to allow internal peers to communicate locally while registered to external LDAP servers. For such search responses, xlates are searched first, and then DNAT entries to obtain the correct address. If both of these searches fail, then the address is not changed. For sites using NAT 0 (no NAT) and not expecting DNAT interaction, we recommend that the inspection engine be turned off to provide better performance.

Additional configuration may be necessary when the ILS server is located inside the security appliance border. This would require a hole for outside clients to access the LDAP server on the specified port, typically TCP 389.

Because ILS traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the TCP inactivity interval. By default, this interval is 60 minutes and can be adjusted using the **timeout** command.

ILS/LDAP follows a client/server model with sessions handled over a single TCP connection. Depending on the client's actions, several of these sessions may be created.

During connection negotiation time, a BIND PDU is sent from the client to the server. Once a successful BIND RESPONSE from the server is received, other operational messages may be exchanged (such as ADD, DEL, SEARCH, or MODIFY) to perform operations on the ILS Directory. The ADD REQUEST and SEARCH RESPONSE PDUs may contain IP addresses of NetMeeting peers, used by H.323 (SETUP and CONNECT messages) to establish the NetMeeting sessions. Microsoft NetMeeting v2.X and v3.X provides ILS support.

The ILS inspection performs the following operations:

- Decodes the LDAP REQUEST/RESPONSE PDUs using the BER decode functions
- Parses the LDAP packet
- Extracts IP addresses
- Translates IP addresses as necessary
- Encodes the PDU with translated addresses using BER encode functions
- Copies the newly encoded PDU back to the TCP packet
- Performs incremental TCP checksum and sequence number adjustment

ILS inspection has the following limitations:

- Referral requests and responses are not supported
- Users in multiple directories are not unified
- Single users having multiple identities in multiple directories cannot be recognized by NAT

Note Because H225 call signalling traffic only occurs on the secondary UDP channel, the TCP connection is disconnected after the interval specified by the TCP **timeout** command. By default, this interval is set at 60 minutes.

Examples

You enable the ILS inspection engine as shown in the following example, which creates a class map to match ILS traffic on the default port (389). The service policy is then applied to the outside interface.

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

To enable ILS inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug ils	Enables debug information for ILS.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect ipsec-pass-thru

To enable ESP inspection, use the **inspect ipsec-pass-thru** 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 ipsec-pass-thru

no inspect ipsec-pass-thru

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(5)	This command was introduced.

Usage Guidelines

This inspection is configured to open pinholes for ESP traffic. All ESP data flows are permitted when a forward flow exists, and there is no limit on the maximum number of connections that can be allowed. AH is not permitted. The default idle timeout for ESP data flows is by default set to 10 minutes. This inspection can be applied in all locations that other inspections can be applied, including class and match command modes.

IPSec Pass Through application inspection provides convenient traversal of ESP (IP protocol 50) traffic associated with an IKE UDP port 500 connection. It avoids lengthy access list configuration to permit ESP traffic and also provides security using timeout and max connections.

Use **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces. The **inspect IPSec-pass-thru** command, when enabled, allows unlimited ESP traffic with a timeout of 10 minutes, which is not configurable.

NAT and non-NAT traffic is permitted. However, PAT is not supported.

Examples

The following example shows how to use an access list to identify IKE traffic, define an IPSec Pass Through policy map, and apply the policy to the outside inteface:

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-cmap)# match access-list test-udp-acl
hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
```

```
hostname(config-pmap-c)# inspect ipsec-pass-thru
hostname(config)# service-policy test-udp-policy interface outside
```

To enable ESP 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 mgcp

To enable MGCP application inspection or to change the ports to which the security appliance listens, use the **inspect mgcp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

Syntax Description

map_name	(Optional) The name of the MGCP map.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

To use MGCP, you usually need to configure at least two **inspect** commands: one for the port on which the gateway receives commands, and one for the port on which the Call Agent receives commands. Normally, a Call Agent sends commands to the default MGCP port for gateways, 2427, and a gateway sends commands to the default MGCP port for Call Agents, 2727.

MGCP is used for controlling media gateways from external call control elements called media gateway controllers or call agents. A media gateway is typically a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks. Using NAT and PAT with MGCP lets you support a large number of devices on an internal network with a limited set of external (global) addresses.

Examples of media gateways are:

- Trunking gateways, that interface between the telephone network and a Voice over IP network. Such gateways typically manage a large number of digital circuits.
- Residential gateways, that provide a traditional analog (RJ11) interface to a Voice over IP network. Examples of residential gateways include cable modem/cable set-top boxes, xDSL devices, broad-band wireless devices.

- Business gateways, that provide a traditional digital PBX interface or an integrated soft PBX interface to a Voice over IP network.

MGCP messages are transmitted over UDP. A response is sent back to the source address (IP address and UDP port number) of the command, but the response may not arrive from the same address as the command was sent to. This can happen when multiple call agents are being used in a failover configuration and the call agent that received the command has passed control to a backup call agent, which then sends the response.

Note MGCP call agents send AUEP messages to determine if MGCP end points are present. This establishes a flow through the security appliance and allows MGCP end points to register with the call agent.

Use the **call-agent** and **gateway** commands in MGCP map configuration mode to configure the IP addresses of one or more call agents and gateways. Use the **command-queue** command in MGCP map configuration mode to specify the maximum number of MGCP commands that will be allowed in the command queue at one time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect mgcp** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect mgcp** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect mgcp** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

The following example shows how to identify MGCP traffic, define a MGCP map, define a policy, and apply the policy to the outside interface. This creates a class map to match MGCP traffic on the default ports (2427 and 2727). The service policy is then applied to the outside interface.

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

This configuration allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117. The maximum number of MGCP commands that can be queued is 150.

To enable MGCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays information about MGCP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect netbios

To enable NetBIOS application inspection or to change the ports to which the security appliance listens, use the **inspect netbios command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect netbios

no inspect netbios

Syntax Description

This command has no arguments or keywords.

Syntax Description

port	The port on which to enable application inspection. You can use port numbers or supported port literals. See Appendix D, "Addresses, Protocols, and Ports," in the *Cisco Security Appliance Command Line Configuration Guide* for a list of valid port literal names.
port-*port*	Specifies a port range.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect netbios** command enables or disables application inspection for the NetBIOS protocol.

Examples

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 security appliance listens, use the **inspect pptp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

```
inspect pptp

no inspect pptp
```

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The Point-to-Point Tunneling Protocol (PPTP) is a protocol for tunneling PPP traffic. A PPTP session is composed of one TCP channel and usually two PPTP GRE tunnels. The TCP channel is the control channel used for negotiating and managing the PPTP GRE tunnels. The GRE tunnels carries PPP sessions between the two hosts.

When enabled, PPTP application inspection inspects PPTP protocol packets and dynamically creates the GRE connections and xlates necessary to permit PPTP traffic. Only Version 1, as defined in RFC 2637, is supported.

PAT is only performed for the modified version of GRE [RFC 2637] when negotiated over the PPTP TCP control channel. Port Address Translation is *not* performed for the unmodified version of GRE [RFC 1701, RFC 1702].

Specifically, the security appliance inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing-call request and reply sequence are tracked. Connections and xlates are dynamic allocated as necessary to permit subsequent secondary GRE data traffic.

The PPTP inspection engine must be enabled for PPTP traffic to be translated by PAT. Additionally, PAT is only performed for a modified version of GRE (RFC2637) and only if it is negotiated over the PPTP TCP control channel. PAT is not performed for the unmodified version of GRE (RFC 1701 and RFC 1702).

As described in RFC 2637, the PPTP protocol is mainly used for the tunneling of PPP sessions initiated from a modem bank PAC (PPTP Access Concentrator) to the headend PNS (PPTP Network Server). When used this way, the PAC is the remote client and the PNS is the server.

However, when used for VPN by Windows, the interaction is inverted. The PNS is a remote single-user PC that initiates connection to the head-end PAC to gain access to a central network. |

Examples

You enable the PPTP inspection engine as shown in the following example, which creates a class map to match PPTP traffic on the default port (1723). The service policy is then applied to the outside interface.

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

To enable PPTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug pptp	Enables debug information for PPTP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect rsh

To enable RSH application inspection or to change the ports to which the security appliance listens, use the **inspect rsh** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rsh

no inspect rsh

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The RSH protocol uses a TCP connection from the RSH client to the RSH server on TCP port 514. The client and server negotiate the TCP port number where the client listens for the STDERR output stream. RSH inspection supports NAT of the negotiated port number if necessary.

Examples

You enable the RSH inspection engine as shown in the following example, which creates a class map to match RSH traffic on the default port (514). The service policy is then applied to the outside interface.

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

To enable RSH inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect rtsp

To enable RTSP application inspection or to change the ports to which the security appliance listens, use the **inspect rtsp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect rtsp

no inspect rtsp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect rtsp** command lets the security appliance pass RTSP packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

Note For Cisco IP/TV, use RTSP TCP port 554 and TCP 8554.

RTSP applications use the well-known port 554 with TCP (rarely UDP) as a control channel. The security appliance only supports TCP, in conformity with RFC 2326. This TCP control channel is used to negotiate the data channels that will be used to transmit audio/video traffic, depending on the transport mode that is configured on the client.

The supported RDT transports are: rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp, and x-pn-tng/udp.

The security appliance parses Setup response messages with a status code of 200. If the response message is travelling inbound, the server is outside relative to the security appliance and dynamic channels need to be opened for connections coming inbound from the server. If the response message is outbound, then the security appliance does not need to open dynamic channels.

Because RFC 2326 does not require that the client and server ports must be in the SETUP response message, the security appliance will need to keep state and remember the client ports in the SETUP message. QuickTime places the client ports in the SETUP message and then the server responds with only the server ports.

Using RealPlayer

When using RealPlayer, it is important to properly configure transport mode. For the security appliance, add an **access-list** command statement from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the security appliance, there is no need to configure the inspection engine.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the security appliance, add a **inspect rtsp** *port* command statement.

Restrictions and Limitations

The following restrictions apply to the **inspect rtsp** command:

- The security appliance does not support multicast RTSP or RTSP messages over UDP.
- PAT is not supported with the **inspect rtsp** command.
- The security appliance does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The security appliance 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 security appliance cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of NATs the security appliance performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.
- Media streams delivered over HTTP are not supported by RTSP application inspection. This is because RTSP inspection does not support HTTP cloaking (RTSP wrapped in HTTP).

Examples

You enable the RTSP inspection engine as shown in the following example, which creates a class map to match RTSP traffic on the default ports (554 and 8554). The service policy is then applied to the outside interface.

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-traffic
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

To enable RTSP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug rtsp	Enables debug information for RTSP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sip

To enable SIP application inspection or to change the ports to which the security appliance listens, use the **inspect sip** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sip

no inspect sip

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment for SIP is 5060.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

SIP, as defined by the IETF, enables VoIP calls. SIP works with SDP for call signalling. SDP specifies the details of the media stream. Using SIP, the security appliance can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP calls through the security appliance, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Also, SIP embeds IP addresses in the user-data portion of the IP packet. SIP inspection applies NAT for these embedded IP addresses.

Note If a remote endpoint tries to register with a SIP proxy on a network protected by the security appliance, the registration will fail under very specific conditions. These conditions are when PAT is configured for the remote endpoint, the SIP registrar server is on the outside network, and when the port is missing in the contact field in the REGISTER message sent by the endpoint to the proxy server.

Instant Messaging

Instant Messaging refers to the transfer of messages between users in near real-time. The MESSAGE/INFO methods and 202 Accept response are used to support IM as defined in the following RFCs:

- Session Initiation Protocol (SIP)-Specific Event Notification, RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging, RFC 3428

MESSAGE/INFO requests can come in at any time after registration/subscription. For example, two users can be online at any time, but not chat for hours. Therefore, the SIP inspection engine opens pinholes, which will time out according to the configured SIP timeout value. This value must be configured at least five minutes longer than the subscription duration. The subscription duration is defined in the Contact Expires value and is typically 30 minutes.

Because MESSAGE/INFO requests are typically sent using a dynamically allocated port other than port 5060, they are required to go through the SIP inspection engine.

Note Only the Chat feature is currently supported. Whiteboard, File Transfer, and Application Sharing are not supported. RTC Client 5.0 is not supported.

Technical Details

SIP inspection NATs the SIP text-based messages, recalculates the content length for the SDP portion of the message, and recalculates the packet length and checksum. It dynamically opens media connections for ports specified in the SDP portion of the SIP message as address/ports on which the endpoint should listen.

SIP inspection has a database with indices CALL_ID/FROM/TO from the SIP payload that identifies the call, as well as the source and destination. Contained within this database are the media addresses and media ports that were contained in the SDP media information fields and the media type. There can be multiple media addresses and ports for a session. RTP/RTCP connections are opened between the two endpoints using these media addresses/ports.

The well-known port 5060 must be used on the initial call setup (INVITE) message. However, subsequent messages may not have this port number. The SIP inspection engine opens signaling connection pinholes, and marks these connections as SIP connections. This is done for the messages to reach the SIP application and be NATed.

As a call is set up, the SIP session is considered in the “transient” state. This state remains until a Response message is received indicating the RTP media address and port on which the destination endpoint is listening. If there is a failure to receive the response messages within one minute, the signaling connection will be torn down.

Once the final handshake is made, the call state is moved to active and the signaling connection will remain until a BYE message is received.

If an inside endpoint initiates a call to an outside endpoint, a media hole is opened to the outside interface to allow RTP/RTCP UDP packets to flow to the inside endpoint media address and media port specified in the INVITE message from the inside endpoint. Unsolicited RTP/RTCP UDP packets to an inside interface will not traverse the security appliance, unless the security appliance configuration specifically allows it.

The media connections are torn down within two minutes after the connection becomes idle. This is, however, a configurable timeout and can be set for a shorter or longer period of time.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect sip** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect sip** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect sip** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the SIP inspection engine as shown in the following example, which creates a class map to match SIP traffic on the default port (5060). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

To enable SIP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
show sip	Displays information about SIP sessions established through the security appliance.
debug sip	Enables debug information for SIP.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect skinny

T o enable SCCP (Skinny) application inspection or to change the ports to which the security appliance listens, use the **inspect skinny** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect skinny

no inspect skinny

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

Skinny (or Simple) Client Control Protocol (SCCP) is a simplified protocol used in VoIP networks. Cisco IP Phones using SCCP can coexist in an H.323 environment. When used with Cisco CallManager, the SCCP client can interoperate with H.323-compliant terminals. Application layer functions in the security appliance recognize SCCP Version 3.3. The functionality of the application layer software ensures that all SCCP signaling and media packets can traverse the security appliance by providing NAT of the SCCP Signaling packets.

There are 5 versions of the SCCP protocol: 2.4, 3.0.4, 3.1.1, 3.2, and 3.3.2. The security appliance supports all versions through Version 3.3.2. The security appliance provides both PAT and NAT support for SCCP. PAT is necessary if you have limited numbers of global IP addresses for use by IP phones.

Normal traffic between the Cisco CallManager and Cisco IP Phones uses SCCP and is handled by SCCP inspection without any special configuration.The security appliance also supports DHCP options 150 and 66, which allow the security appliance to send the location of a TFTP server to Cisco IP Phones and other DHCP clients. For more information, see the **dhcp-server** command.

Supporting Cisco IP Phones

In topologies where Cisco CallManager is located on the higher security interface with respect to the Cisco IP Phones, if NAT is required for the Cisco CallManager IP address, the mapping must be **static** as a Cisco IP Phone requires the Cisco CallManager IP address to be specified explicitly in its configuration. An identity static entry allows the Cisco CallManager on the higher security interface to accept registrations from the Cisco IP Phones.

Cisco IP Phones require access to a TFTP server to download the configuration information they need to connect to the Cisco CallManager server.

When the Cisco IP Phones are on a lower security interface compared to the TFTP server, you must use an access list to connect to the protected TFTP server on UDP port 69. While you do need a static entry for the TFTP server, this does not have to be an "identity" static entry. When using NAT, an identity static entry maps to the same IP address. When using PAT, it maps to the same IP address and port.

When the Cisco IP Phones are on a *higher* security interface compared to the TFTP server and Cisco CallManager, no access list or static entry is required to allow the Cisco IP Phones to initiate the connection.

Restrictions and Limitations

The following are limitations that apply to the current version of PAT and NAT support for SCCP:

- PAT will not work with configurations using the **alias** command.
- Outside NAT or PAT is **not** supported.

Note Stateful Failover of SCCP calls is now supported except for calls that are in the middle of call setup.

If the address of an internal Cisco CallManager is configured for NAT or PAT to a different IP address or port, registrations for external Cisco IP Phones will fail because the security appliance currently does not support NAT or PAT for the file content transferred via TFTP. Although the security appliance does support NAT of TFTP messages, and opens a pinhole for the TFTP file to traverse the security appliance, the security appliance cannot translate the Cisco CallManager IP address and port embedded in the Cisco IP Phone's configuration files that are being transferred using TFTP during phone registration.

Inspecting Signaling Messages

For inspecting signaling messages, the **inspect skinny** command often needs to determine locations of the media endpoints (for example, IP phones).

This information is used to prepare access-control and NAT state for media traffic to traverse the firewall transparently without manual configuration.

In determining these locations, the **inspect skinny** command does **not** use the tunnel default gateway route. A tunnel default gateway route is a route of the form **route** *interface* **0 0** *metric* **tunneled**. This route overrides the default route for packets that egress from IPSec tunnels. Therefore, if the **inspect skinny** command is desired for VPN traffic, do not configure the tunnel default gateway route. Instead, us other static routing or dynamic routing.

Examples

You enable the SCCP inspection engine as shown in the following example, which creates a class map to match SCCP traffic on the default port (2000). The service policy is then applied to the outside interface.

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
```

```
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

To enable SCCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debug information.
show skinny	Displays information about SCCP sessions established through the security appliance.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

inspect snmp

To enable SNMP application inspection or to change the ports to which the security appliance listens, use the **inspect snmp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect snmp *map_name*

no inspect snmp *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the inspect snmp command to enable SNMP inspection, using the settings configured with an SNMP map, which you create using the **snmp-map** command. Use the **deny version** command in SNMP map configuration mode to restrict SNMP traffic to a specific version of SNMP.

Earlier versions of SNMP are less secure so restricting SNMP traffic to Version 2 may be required by your security policy. To deny a specific version of SNMP, use the **deny version** command within an SNMP map, which you create using the **snmp-map** command. After configuring the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example identifies SNMP traffic, defines an SNMP map, defines a policy, enables SNMP inspection, and applies the policy to the outside interface:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
```

```
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

To enable strict snmp application inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect sqlnet

To enable Oracle SQL*Net application inspection, use the **inspect sqlnet** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sqlnet

no inspect sqlnet

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 1521.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The SQL*Net protocol consists of different packet types that the security appliance handles to make the data stream appear consistent to the Oracle applications on either side of the security appliance.

The default port assignment for SQL*Net is 1521. This is the value used by Oracle for SQL*Net, but this value does not agree with IANA port assignments for Structured Query Language (SQL). Use the **class-map** command to apply SQL*Net inspection to a range of port numbers.

Note Disable SQL*Net inspection when SQL data transfer occurs on the same port as the SQL control TCP port 1521. The security appliance acts as a proxy when SQL*Net inspection is enabled and reduces the client window size from 65000 to about 16000 causing data transfer issues.

The security appliance NATs all addresses and looks in the packets for all embedded ports to open for SQL*Net Version 1.

For SQL*Net Version 2, all DATA or REDIRECT packets that immediately follow REDIRECT packets with a zero data length will be fixed up.

The packets that need fix-up contain embedded host/port addresses in the following format:

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net Version 2 TNSFrame types (Connect, Accept, Refuse, Resend, and Marker) will not be scanned for addresses to NAT nor will inspection open dynamic connections for any embedded ports in the packet.

SQL*Net Version 2 TNSFrames, Redirect, and Data packets will be scanned for ports to open and addresses to NAT, if preceded by a REDIRECT TNSFrame type with a zero data length for the payload. When the Redirect message with data length zero passes through the security appliance, a flag will be set in the connection data **S**tructure to expect the Data or Redirect message that follows to be NATed and ports to be dynamically opened. If one of the TNS frames in the preceding paragraph arrive after the Redirect message, the flag will be reset.

The SQL*Net inspection engine will recalculate the checksum, change IP, TCP lengths, and readjust Sequence Numbers and Acknowledgment Numbers using the delta of the length of the new and old message.

SQL*Net Version 1 is assumed for all other cases. TNSFrame types (Connect, Accept, Refuse, Resend, Marker, Redirect, and Data) and all packets will be scanned for ports and addresses. Addresses will be NATed and port connections will be opened.

Examples

You enable the SQL*Net inspection engine as shown in the following example, which creates a class map to match SQL*Net traffic on the default port (1521). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

To enable SQL*Net inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug sqlnet	Enables debug information for SQL*Net.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types, including SQL*net.

inspect sunrpc

To enable Sun RPC application inspection or to change the ports to which the security appliance listens, use the **inspect sunrpc** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect sunrpc

no inspect sunrpc

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the **fixup** command, which is now deprecated.

Usage Guidelines

To enable Sun RPC application inspection or to change the ports to which the security appliance listens, use the **inspect sunrpc** command in policy map class configuration mode, which is accessible by using the **class** command within policy map configuration mode. To remove the configuration, use the **no** form of this command.

The **inspect sunrpc** command enables or disables application inspection for the Sun RPC protocol. Sun RPC is used by NFS and NIS. Sun RPC services can run on any port on the system. When a client attempts to access an Sun RPC service on a server, it must find out which port that service is running on. It does this by querying the portmapper process on the well-known port of 111.

The client sends the Sun RPC program number of the service, and gets back the port number. From this point on, the client program sends its Sun RPC queries to that new port. When a server sends out a reply, the security appliance intercepts this packet and opens both embryonic TCP and UDP connections on that port.

Note NAT or PAT of Sun RPC payload information is not supported.

Examples

You enable the RPC inspection engine as shown in the following example, which creates a class map to match RPC traffic on the default port (111). The service policy is then applied to the outside interface.

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

To enable RPC inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
clear configure sunrpc_server	Removes the configuration performed using the **sunrpc-server** command.
clear sunrpc-server active	Clears the pinholes that are opened by Sun RPC application inspection for specific services, such as NFS or NIS.
show running-config sunrpc-server	Displays the information about the Sun RPC service table configuration.
sunrpc-server	Allows pinholes to be created with a specified timeout for Sun RPC services, such as NFS or NIS.
show sunrpc-server active	Displays the pinholes open for Sun RPC services.

inspect tftp

To disable TFTP application inspection, or to enable it if it has been previously disabled, use the **inspect tftp** command in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect tftp

no inspect tftp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

The default port assignment is 69.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

Trivial File Transfer Protocol (TFTP), described in RFC 1350, is a simple protocol to read and write files between a TFTP server and client.

The security appliance inspects TFTP traffic and dynamically creates connections and translations, if necessary, to permit file transfer between a TFTP client and server. Specifically, the inspection engine inspects TFTP read request (RRQ), write request (WRQ), and error notification (ERROR).

A dynamic secondary channel and a PAT translation, if necessary, are allocated on a reception of a valid read (RRQ) or write (WRQ) request. This secondary channel is subsequently used by TFTP for file transfer or error notification.

Only the TFTP server can initiate traffic over the secondary channel, and at most one incomplete secondary channel can exist between the TFTP client and server. An error notification from the server closes the secondary channel.

TFTP inspection must be enabled if static PAT is used to redirect TFTP traffic.

Examples

You enable the TFTP inspection engine as shown in the following example, which creates a class map to match TFTP traffic on the default port (69). The service policy is then applied to the outside interface.

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

To enable TFTP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

inspect xdmcp

To enable XDMCP application inspection or to change the ports to which the security appliance listens, use the **inspect xdmcp command** in class configuration mode. Class configuration mode is accessible from policy map configuration mode. To remove the configuration, use the **no** form of this command.

inspect xdmcp

no inspect xdmcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced, replacing the previously existing **fixup** command, which is now deprecated.

Usage Guidelines

The **inspect xdmcp** command enables or disables application inspection for the XDMCP protocol.

XDMCP is a protocol that uses UDP port 177 to negotiate X sessions, which use TCP when established.

For successful negotiation and start of an XWindows session, the security appliance must allow the TCP back connection from the Xhosted computer. To permit the back connection, use the **established** command on the security appliance. Once XDMCP negotiates the port to send the display, The **established** command is consulted to verify if this back connection should be permitted.

During the XWindows session, the manager talks to the display Xserver on the well-known port 6000 | n. Each display has a separate connection to the Xserver, as a result of the following terminal setting.

```
setenv DISPLAY Xserver:n
```

where *n* is the display number.

When XDMCP is used, the display is negotiated using IP addresses, which the security appliance can NAT if needed. XDCMP inspection does not support PAT.

Examples

You enable the XDMCP inspection engine as shown in the following example, which creates a class map to match XDMCP traffic on the default port (177). The service policy is then applied to the outside interface.

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

To enable XDMCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug xdmcp	Enables debug information for XDMCP.
policy-map	Associates a class map with specific security actions.
service-policy	Applies a policy map to one or more interfaces.

intercept-dhcp

To enable DHCP Intercept, use the **intercept-dhcp enable** command in group-policy configuration mode. To disable DHCP Intercept, use the **intercept-dhcp disable** command.

To remove the intercept-dhcp attribute from the running configuration, use the **no intercept-dhcp** command. This lets users inherit a DHCP Intercept configuration from the default or other group policy.

DHCP Intercept lets Microsoft XP clients use split-tunneling with the security appliance. The security appliance replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

Syntax Description

disable	Disables DHCP Intercept.
enable	Enables DHCP Intercept.
netmask	Provides the subnet mask for the tunnel IP address.

Defaults

DHCP Intercept is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the security appliance limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

Examples

The following example shows how to set DHCP Intercept S for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

interface

To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode. To create a logical subinterface, use the *subinterface* argument. To remove a subinterface, use the **no** form of this command; you cannot remove a physical interface. In interface configuration mode, you can configure hardware settings, assign a name, assign a VLAN, assign an IP address, and configure many other settings.

interface {*physical_interface*[**.***subinterface*] | *mapped_name*}

no interface *physical_interface***.***subinterface*

Syntax Description

mapped_name	In multiple context mode, enter the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	The physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional. The physical interface types include the following: • **ethernet** • **gigabitethernet** For the PIX 500 series security appliance, enter the type followed by the port number, for example, **ethernet0**. For the ASA 5500 series adaptive security appliance, enter the type followed by slot/port, for example, **gigabitethernet0/1**. Interfaces that are built into the chassis are assigned to slot 0, while interfaces on the 4GE SSM are assigned to slot 1. The ASA 5500 series adaptive security appliance also includes the following type: • **management** The management interface is a Fast Ethernet interface designed for management traffic only, and is specified as **management0/0**. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode. See the hardware documentation that came with your model to identify the interface type, slot, and port number.
subinterface	(Optional) An integer between 1 and 4294967293 designating a logical subinterface. The maximum number of subinterfaces varies depending on your security appliance model. See the *Cisco Security Appliance Command Line Configuration Guide* for the maximum subinterfaces per platform.

Defaults

By default, the security appliance automatically generates **interface** commands for all physical interfaces.

In multiple context mode, the security appliance automatically generates **interface** commands for all interfaces allocated to the context using the **allocate-interface** command.

All physical interfaces are shut down by default. Allocated interfaces in contexts are not shut down in the configuration.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified to allow for new subinterface naming conventions and to change arguments to be separate commands under interface configuration mode.

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.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For subinterfaces, configure the **vlan** command. The security level is 0 (lowest) by default. See the **security-level** command for default levels for some interfaces or to change from the default of 0 so interfaces can communicate with each other.

The ASA adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Note Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA adaptive security appliance, you can use the dedicated management interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

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

You cannot delete the physical interfaces using the **no** form of the **interface** command, nor can you delete the allocated interfaces within a context.

In multiple context mode, you configure physical parameters, subinterfaces, and VLAN assignments in the system configuration only. You configure other parameters in the context configuration only.

Examples

The following example configures parameters for the physical interface in single mode:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example configures parameters for a subinterface in single mode:

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

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 (vpn load-balancing)

To specify a non-default public or private interface for VPN load-balancing in the VPN load-balancing virtual cluster, use the **interface** command in vpn load-balancing mode. To remove the interface specification and revert to thte default interface, use the **no** form of this command.

interface {**lbprivate** | **lbpublic**} *interface-name*]

no interface {**lbprivate** | **lbpublic**}

Syntax Description

interface-name	The name of the interface to be configured as the public or private interface for the VPN load-balancing cluster.
lbprivate	Specifies that this command configures the private interface for VPN load-balancing.
lbpublic	Specifies that this command configures the public interface for VPN load-balancing.

Defaults

If you omit the **interface** command, the **lbprivate** interface defaults to **inside**, and the **lbpublic** interface defaults to **outside**.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must have first used the **vpn load-balancing** command to enter vpn load-balancing mode.

You must also have previously used the **interface**, **ip address**, and **nameif** commands to configure and assign a name to the interface that you are specifying in this command.

The no form of this command reverts the interface to its default.

Examples

The following is an example of a **vpn load-balancing** command sequence that includes an **interface** command that specifies the public interface of the cluster as “test” one that reverts the private interface of the cluster to the default (inside):

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
```

```
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **interface-policy** command in failover group configuration mode. To restore the default values, use the **no** form of this command.

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

If the **failover interface-policy** command is configured for the unit, then the default for the **interface-policy** failover group command assumes that value. If not, then *num* is 1.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other security appliance is functioning properly, the security appliance will mark itself as failed and a failover may occur (if the active security appliance is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Examples

The following partial example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover interface-policy	Configures the interface monitoring policy.
monitor-interface	Specifies the interfaces being monitored for failover.

ip-address

To include the security appliance IP address in the certificate during enrollment, use the **ip-addr** 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

ip-address	Specifies the IP address of the security appliance.

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the security appliance IP address in the enrollment request for trustpoint central:

```
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

To set the IP address for an interface (in routed mode) or for the management address (transparent mode), use the **ip address** command. For routed mode, enter this command in interface configuration mode. In transparent mode, enter this command in global configuration mode. To remove the IP address, use the **no** form of this command. This command also sets the standby address for failover.

ip address *ip_address* [*mask*] [**standby** *ip_address*]

no ip address [*ip_address*]

Syntax Description

ip_address	The IP address for the interface (routed mode) or the management IP address (transparent mode).
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
standby *ip_address*	(Optional) The IP address for the standby unit for failover.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is to set the management IP address. This address is required because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

The following example sets the management address and standby address of a transparent firewall:

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
show ip address	Shows the IP address assigned to an interface.

ip address dhcp

To use DHCP to obtain an IP address for an interface, use the **ip address dhcp** command in interface configuration mode. To disable the DHCP client for this interface, use the **no** form of this command.

ip address dhcp [**setroute**]

no ip address dhcp

Syntax Description

setroute	(Optional) Allows the security appliance to use the default route supplied by the DHCP server.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from a global configuration command to an interface configuration mode command. You can also enable this command on any interface, instead of only the outside interface.

Usage Guidelines

Reenter this command to reset the DHCP lease and request a new lease.

You cannot set this command at the same time as the **ip address** command.

If you enable the **setroute** option, do not configure a default route using the **route** command.

If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

Note The security appliance rejects any leases that have a timeout of less than 32 seconds.

Examples

The following example enables DHCP on the gigabitethernet0/1 interface:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
show ip address dhcp	Shows the IP address obtained from the DHCP server.

ip audit attack

To set the default actions for packets that match an attack signature, use the **ip audit attack** command in global configuration mode. To restore the default action (to reset the connection), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to send and alarm.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an attack signature. The audit policy for the inside interface overrides this default to be alarm only, while the policy for the outside interface uses the default setting set with the **ip audit attack** command.

```
hostname(config)# ip audit attack action alarm reset
```

```
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

ip audit info

To set the default actions for packets that match an informational signature, use the **ip audit info** command in global configuration mode. To restore the default action (to generate an alarm), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to generate an alarm.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an informational signature. The audit policy for the inside interface overrides this default to be alarm and drop, while the policy for the outside interface uses the default setting set with the **ip audit info** command.

```
hostname(config)# ip audit info action alarm reset
```

```
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit info	Shows the configuration for the **ip audit info** command.

ip audit interface

To assign an audit policy to an interface, use the **ip audit interface** command in global configuration mode. To remove the policy from the interface, use the **no** form of this command.

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

Syntax Description

interface_name	Specifies the interface name.
policy_name	The name of the policy you added with the **ip audit name** command. You can assign an **info** policy and an **attack** policy to each interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example applies audit policies to the inside and outside interfaces:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.

Command	Description
ip audit signature	Disables a signature.
show running-config ip audit interface	Shows the configuration for the **ip audit interface** command.

ip audit name

To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the **ip audit name** command in global configuration mode. Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. To remove the policy, use the **no** form of this command.

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

Syntax Description

action	(Optional) Specifies that you are defining a set of actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, then the security appliance uses the default action set by the **ip audit attack** and **ip audit info** commands.
alarm	(Optional) Generates a system message showing that a packet matched a signature.
attack	Creates an audit policy for attack signatures; the packet might be part of an attack on your network, such as a DoS attack or illegal FTP commands.
drop	(Optional) Drops the packet.
info	Creates an audit policy for informational signatures; the packet is not currently attacking your network, but could be part of an information-gathering activity, such as a port sweep.
name	Sets the name of the policy.
reset	(Optional) Drops the packet and closes the connection.

Defaults

If you do not change the default actions using the **ip audit attack** and **ip audit info** commands, then the default action for attack signatures and informational signatures is to generate an alarm.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To apply the policy, assign it to an interface using the **ip audit interface** command. You can assign an **info** policy and an **attack** policy to each interface.

For a list of signatures, see the **ip audit signature** command.

If traffic matches a signature, and you want to take action against that traffic, use the **shun** command to prevent new connections from the offending host and to disallow packets from any existing connection.

Examples

The following example sets an audit policy for the inside interface to generate an alarm for attack and informational signatures, while the policy for the outside interface resets the connection for attacks:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
shun	Blocks packets with a specific source and destination address.

ip audit signature

To disable a signature for an audit policy, use the **ip audit signature** command in global configuration mode. To reenable the signature, use the **no** form of this command. You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms.

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

Syntax Description

signature_number	Specifies the signature number to disable. See Table 5-4 for a list of supported signatures.
disable	Disables the signature.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Table 5-4 lists supported signatures and system message numbers.

Table 5-4 Signature IDs and System Message Numbers

Signature ID	Message Number	Signature Title	Signature Type	Description
1000	400000	IP options-Bad Option List	Informational	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001	400001	IP options-Record Packet Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).

Table 5-4 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
1002	400002	IP options-Timestamp	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003	400003	IP options-Security	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004	400004	IP options-Loose Source Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005	400005	IP options-SATNET ID	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006	400006	IP options-Strict Source Route	Informational	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100	400007	IP Fragment Attack	Attack	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
1102	400008	IP Impossible Packet	Attack	Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1103	400009	IP Overlapping Fragments (Teardrop)	Attack	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.
2000	400010	ICMP Echo Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
2001	400011	ICMP Host Unreachable	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).

Table 5-4 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2002	400012	ICMP Source Quench	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
2003	400013	ICMP Redirect	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004	400014	ICMP Echo Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005	400015	ICMP Time Exceeded for a Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006	400016	ICMP Parameter Problem on Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
2007	400017	ICMP Timestamp Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
2008	400018	ICMP Timestamp Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009	400019	ICMP Information Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010	400020	ICMP Information Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011	400021	ICMP Address Mask Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012	400022	ICMP Address Mask Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).

Table 5-4 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2150	400023	Fragmented ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.
2151	400024	Large ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
2154	400025	Ping of Death Attack	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3040	400026	TCP NULL flags	Attack	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3041	400027	TCP SYN+FIN flags	Attack	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3042	400028	TCP FIN only flags	Attack	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3153	400029	FTP Improper Address Specified	Informational	Triggers if a port command is issued with an address that is not the same as the requesting host.
3154	400030	FTP Improper Port Specified	Informational	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
4050	400031	UDP Bomb attack	Attack	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
4051	400032	UDP Snork attack	Attack	Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052	400033	UDP Chargen DoS attack	Attack	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
6050	400034	DNS HINFO Request	Informational	Triggers on an attempt to access HINFO records from a DNS server.

Table 5-4 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6051	400035	DNS Zone Transfer	Informational	Triggers on normal DNS zone transfers, in which the source port is 53.
6052	400036	DNS Zone Transfer from High Port	Informational	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053	400037	DNS Request for All Records	Attack	Triggers on a DNS request for all records.
6100	400038	RPC Port Registration	Informational	Triggers when attempts are made to register new RPC services on a target host.
6101	400039	RPC Port Unregistration	Informational	Triggers when attempts are made to unregister existing RPC services on a target host.
6102	400040	RPC Dump	Informational	Triggers when an RPC dump request is issued to a target host.
6103	400041	Proxied RPC Request	Attack	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153	400045	ypupdated (YP update daemon) Portmap Request	Attack	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Attack	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155	400047	mountd (mount daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.

Table 5-4 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6180	400049	rexd (remote execution daemon) Attempt	Informational	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
6190	400050	statd Buffer Overflow	Attack	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Examples

The following example disables signature 6100:

```
hostname(config)# ip audit signature 6100 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit signature	Shows the configuration for the **ip audit signature** command.

ip local pool

To configure IP address pools to be used for VPN remote access tunnels, use the **ip local pool** command in global configuration mode. To delete address pools, use the **no** form of this command.

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

Syntax Description

first-address	Specifies the starting address in the range of IP addresses.
last-address	Specifies the final address in the range of IP addresses.
mask *mask*	(Optional) Specifies a subnet mask for the pool of addresses.
poolname	Specifies the name of the IP address pool.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must supply the mask value when the IP addresses assigned to VPN clients belong to a non-standard network and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets fall under the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

Examples

The following example configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools.
show running-config ip local pool	Displays the ip pool configuration. To specify a specific IP address pool, include the name in the command.

ip-comp

To enable LZS IP compression, use the **ip-comp enable** command in group-policy configuration mode. To disable IP compression, use the **ip-comp disable** command.

To remove the **ip-comp** attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value from another group policy.

ip-comp {**enable** | **disable**}

no ip-comp

Syntax Description

disable	Disables IP compression.
enable	Enables IP compression.

Defaults

IP compression is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.

Caution Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the security appliance. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

Examples

The following example shows how to enable IP compression for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode. To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for IP Phone Bypass from another group policy.

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. If enabled, secure unit authentication remains in effect.

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

Syntax Description

disable	Disables IP Phone Bypass.
enable	Enables IP Phone Bypass.

Defaults

IP Phone Bypass is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You need to configure IP Phone Bypass only if you have enabled user authentication.

Examples

The following example shows how to enable IP Phone Bypass. for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

Related Commands

Command	Description
user-authentication	Requires users behind a hardware client to identify themselves to the security appliance before connecting.

ips

The ASA 5500 series adaptive security appliance supports the AIP SSM, which runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

To assign traffic from the security appliance to the AIP SSM, use the **ips** command in class configuration mode. To remove this command, use the **no** form of this command.

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**}

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**}

Syntax Description

fail-close	Blocks traffic if the AIP SSM fails.
fail-open	Permits traffic if the AIP SSM fails.
inline	Directs packets to the AIP SSM; the packet might be dropped as a result of IPS operation.
promiscuous	Duplicates packets for the AIP SSM; the original packet cannot be dropped by the AIP SSM.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To configure the **ips** command, you must first configure the **class-map** command, **policy-map** command and the **class** command.

After you configure the security appliance to divert traffic to the AIP SSM, configure the AIP SSM inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. You can either session to the AIP SSM from the security appliance (the **session** command) or you can connect directly to the AIP SSM using SSH or Telnet on its mangement interface. Alternatively, you can use ASDM. For more information about configuring the AIP SSM, see *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

Examples

The following example diverts all IP traffic to the AIP SSM in promiscous mode, and blocks all IP traffic should the AIP SSM card fail for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
clear configure policy-map	Removes all **policy-map** configuration, except that if a policy map is in use in a **service-policy** command, that policy map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current **policy-map** configurations.

ipsec-udp

To enable IPSec over UDP, use the **ipsec-udp enable** command in group-policy configuration mode. To disable IPSec over UDP, use the **ipsec-udp disable** command. To remove the IPSec over UDP attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for IPSec over UDP from another group policy.

IPSec over UDP, sometimes called IPSec through NAT, lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ipsec-udp {enable | disable}

no ipsec-udp

Syntax Description

disable	Disables IPSec over UDP.
enable	Enables IPSec over UDP.

Defaults

IPSec over UDP is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

To use IPSec over UDP, you must also configure the **ipsec-udp-port** command.

The Cisco VPN Client must also be configured to use IPSec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPSec over UDP.

IPSec over UDP is proprietary, it applies only to remote-access connections, and it requires mode configuration, means the security appliance exchanges configuration parameters with the client while negotiating SAs.

Using IPSec over UDP may slightly degrade system performance.

Examples

The following example shows how to set IPSec over UDP for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

Related Commands

Command	Description
ipsec-udp-port	Specifies the port on which the security appliance listens for UDP traffic.

ipsec-udp-port

To set a UDP port number for IPSec over UDP, use the **ipsec-udp-port** command in group-policy configuration mode. To disable the UDP port, use the **no** form of this command. This enables inheritance of a value for the IPSec over UDP port from another group policy.

In IPSec negotiations. the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic.

ipsec-udp-port *port*

no ipsec-udp-port

Syntax Description

port	Identifies the UDP port number using an integer in the range 4001 through 49151.

Defaults

The default port is 10000.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can configure multiple group policies with this feature enabled, and each group policy can use a different port number.

Examples

The following example shows how to set an IPSec UDP port to port 4025 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

Command	Description
ipsec-udp	Lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ip verify reverse-path

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. To disable this feature, use the **no** form of this command. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

Syntax Description

interface_name	The interface on which you want to enable Unicast RPF.

Defaults

This feature is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Normally, the security appliance only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the security appliance to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the security appliance can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the security appliance uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.

- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

Examples

The following example enables Unicast RPF on the outside interface:

```
hostname(config)# ip verify reverse-path interface outside
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

ipv6 access-list

To configure an IPv6 access list, use the **ipv6 access-list** command in global configuration mode. To remove an ACE, use the **no** form of this command. Access lists define the traffic that the security appliance allows to pass through or blocks.

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

Syntax Description

any	An abbreviation for the IPv6 prefix ::/0, indicating any IPv6 address.
default	(Optional) Specifies that a syslog message 106100 is generated for the ACE.
deny	Denies access if the conditions are matched.
destination-ipv6-address	The IPv6 address of the host receiving the traffic.
destination-ipv6-prefix	The IPv6 network address where the traffic is destined.
disable	(Optional) Disables syslog messaging.
host	Indicates that the address refers to a specific host.
icmp6	Specifies that the access rule applies to ICMPv6 traffic passing through the security appliance.

icmp_type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect Omitting the *icmp_type* argument indicates all ICMP types.
icmp_type_obj_grp_id	(Optional) Specifies the object group ICMP type ID.
id	Name or number of an access list.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds. The default interval is 300 seconds. This value is also used as the timeout value for deleting an inactive flow.
level	(Optional) Specifies the syslog level for message 106100; valid values are from 0 to 7. The default level is 6 (informational).
line *line-num*	(Optional) The line number where the access rule is being inserted into the list. If you do not specify a line number, the ACE is added to the end of the access list.
log	(Optional) Specifies the logging action for the ACE. If you do not specify the **log** keyword or you specify the **log default** keyword, then message 106023 is generated when a packet is denied by the ACE. If you sepcify the log keyword alone or with a level or interval, then message 106100 is generated when a packet is denied by the ACE. Packets that are denied by the implicit deny at the end of an access list are not logged. You must explicitly deny packets with an ACE to enable logging.
network_obj_grp_id	Existing network object group identification.
object-group	(Optional) Specifies an object group.

operator	(Optional) Specifies the operand to compare the source IP address to the destination IP address. The *operator* compares the source IP address or destination IP address ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **ipv6 access-list** command without an operator and port to indicate all ports by default.
permit	Permits access if the conditions are matched.
port	(Optional) Specifies the port that you permit or deny access. When entering the *port* argument, you can specify the port by either a number in the range of 0 to 65535 or a using literal name if the *protocol* is **tcp** or **udp**. Permitted TCP literal names are **aol, bgp**, **chargen**, **cifc**, **citrix-ica**, **cmd**, **ctiqbe**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **https**, **ident**, **irc**, **kerberos**, **klogin**, **kshell**, **ldap**, **ldaps**, **login**, **lotusnotes**, **lpd**, **netbios-ssn**, **nntp**, **pop2**, **pop3**, **pptp**, **rsh**, **rtsp**, **smtp**, **sqlnet**, **ssh**, **sunrpc, tacacs, talk, telnet, uucp, whois, and www**. Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **cifs**, **discard**, **dnsix**, **domain**, **echo**, **http**, **isakmp**, **kerberos**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **ntp**, **pcanywhere-status**, **pim-auto-rp**, **radius**, **radius-acct**, **rip**, **secureid-udp**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, **www**, and **xdmcp**.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
protocol	Name or number of an IP protocol; valid values are **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number.
protocol_obj_grp_id	Existing protocol object group identification.
service_obj_grp_id	(Optional) Specifies the object group.
source-ipv6-address	The IPv6 address of the host sending the traffic.
source-ipv6-prefix	The IPv6 network address of the where the network traffic originated.

Defaults

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

The default logging interval is 300 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command allows you to specify if an IPv6 address is permitted or denied access to a port or protocol. Each command is called an ACE. One or more ACEs with the same access list name are referred to as an access list. Apply an access list to an interface using the **access-group** command.

The security appliance denies all packets from an outside interface to an inside interface unless you specifically permit access using an access list. All packets are allowed by default from an inside interface to an outside interface unless you specifically deny access.

The **ipv6 access-list** command is similar to the **access-list** command, except that it is IPv6-specific. For additional information about access lists, refer to the **access-list extended** command.

The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the security appliance.To configure the ICMPv6 traffic that is allowed to originate and terminate at a specific interface, use the **ipv6 icmp** command.

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

Examples

The following example will allow any host using TCP to access the 3001:1::203:A0FF:FED6:162D server:

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
```

The following example uses **eq** and a port to deny access to just FTP:

```
hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp
hostname(config)# access-group acl_out in interface inside
```

The following example uses **lt** to permit access to all ports less than port 2025, which permits access to the well-known ports (1 to 1024):

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host 3001:1::203:A0FF:FED6:162D
lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

Related Commands

Command	Description
access-group	Assigns an access list to an interface.
ipv6 icmp	Configures access rules for ICMP messages that terminate at an interface of the security appliance.
object-group	Creates an object group (addresses, ICMP types, and services).

ipv6 address

To enable IPv6 and configure the IPv6 addresses on an interface, use the **ipv6 address** command in interface configuration mode. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

no ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

Syntax Description

autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface.
eui-64	(Optional) Specifies an interface ID in the low order 64 bits of the IPv6 address.
ipv6-address	The IPv6 link-local address assigned to the interface.
ipv6-prefix	The IPv6 network address assigned to the interface.
link-local	Specifies that the address is a link-local address.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).

Defaults

IPv6 is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Configuring an IPv6 address on an interface enables IPv6 on that interface; you do not need to use the **ipv6 enable** command after specifying an IPv6 address.

The **ipv6 address autoconfig** command is used to enable automatic configuration of IPv6 addresses on an interface using stateless autoconfiguration. The addresses are configured based on the prefixes received in Router Advertisement messages. If a link-local address has not been configured, then one is automatically generated for this interface. An error message is displayed if another host is using the link-local address.

The **ipv6 address eui-64** command is used to configure an IPv6 address for an interface. If the optional **eui-64** is specified, the EUI-64 interface ID will be used in the low order 64 bits of the address. If the value specified for the *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID. An error message will be displayed if another host is using the specified address.

The Modified EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64 bit interface ID of 02E0:B6FF:FE01:3B7A.

The **ipv6 address link-local** command is used to configure an IPv6 link-local address for an interface. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface. The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in Modified EUI-64 format. An interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error message will be displayed if another host is using the specified address.

Examples

The following example assigns 3FFE:C00:0:1::576/64 as the global address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

The following example assigns an IPv6 address automatically for the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

The following example assigns IPv6 address 3FFE:C00:0:1::/64 to the selected interface and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

Related Commands

Command	Description
debug ipv6 interface	Displays debug information for IPv6 interfaces.
show ipv6 interface	Displays the status of interfaces configured for IPv6.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing.

The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address for an interface and enables IPv6 processing on the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 icmp

To configure ICMP access rules for an interface, use the **ipv6 icmp** command in global configuration mode. To remove an ICMP access rule, use the **no** form of this command.

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

Syntax Description

any	Keyword specifying any IPv6 address. An abbreviation for the IPv6 prefix ::/0.
deny	Prevents the specified ICMP traffic on the selected interface.
host	Indicates that the address refers to a specific host.
icmp-type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	The name of the interface, as designated by the **nameif** command, the access rule applies to.
ipv6-address	The IPv6 address of the host sending ICMPv6 messages to the interface.
ipv6-prefix	The IPv6 network that is sending ICMPv6 messages to the interface.
permit	Allows the specified ICMP traffic on the selected interface.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Defaults

If no ICMP access rules are defined, all ICMP traffic is permitted.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

If there are no ICMP rules defined for an interface, all IPv6 ICMP traffic is permitted.

If there are ICMP rules defined for an interface, then the rules are processed in order on a first-match basis followed by an implicit deny all rule. For example, if the first matched rule is a permit rule, the ICMP packet is processed. If the first matched rule is a deny rule, or if the ICMP packet did not match any rule on that interface, then the security appliance discards the ICMP packet and generates a syslog message.

For this reason, the order that you enter the ICMP rules is important. If you enter a rule denying all ICMP traffic from a specific network, and then follow it with a rule permitting ICMP traffic from a particular host on that network, the host rule will never be processed. The ICMP traffic is blocked by the network rule. However, if you enter the host rule first, followed by the network rule, the host ICMP traffic will be allowed, while all other ICMP traffic from that network is blocked.

The **ipv6 icmp** command configures access rules for ICMP traffic that terminates at the security appliance interfaces. To configure access rules for pass-through ICMP traffic, refer to the **ipv6 access-list** command.

Examples

The following example denies all ping requests and permits all Packet Too Big messages (to support Path MTU Discovery) at the outside interface:

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection, use the **ipv6 nd dad attempts** command in interface configuration mode. To return to the default number of duplicate address detection messages sent, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

Syntax Description

value	A number from 0 to 600. Entering 0 disables duplicate address detection on the specified interface. Entering 1 configures a single transmission without follow-up transmissions. The default value is 1 message.

Defaults

The default number of attempts is 1.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. The frequency at which the neighbor solicitation messages are sent is configured using the **ipv6 nd ns-interval** command.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state.

Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up. An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

Note While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Examples

The following example configures 5 consecutive neighbor solicitation messages to be sent when duplicate address detection is being performed on the tentative unicast IPv6 address of the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

Syntax Description

value	The interval between IPv6 neighbor solicitation transmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds.

Defaults

1000 milliseconds between neighbor solicitation transmissions.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for Gigabitethernet 0/0:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

Syntax Description

at *valid-date preferred-date*	The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire*.
default	Default values are used.
infinite	(Optional) The valid lifetime does not expire.
ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no-advertise	(Optional) Indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is not used for on-link determination.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 604800 (7 days).
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
valid-lifetime	The amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with **infinite**. The default is 2592000 (30 days).

Defaults

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is "on" (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is "on" (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds, in router advertisements sent out on the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	(Optional) indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is seconds.
value	The interval between IPv6 router advertisement transmissions. Valid values range from 3 to 1800 seconds, or from 500 to 1800000 milliseconds if the **msec** keyword is provided. The default is 200 seconds.

Defaults

200 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the security appliance is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

To configure the "router lifetime" value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

Syntax Description

seconds	The validity of the security appliance as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the security appliance should not be considered a default router on the selected interface.

Defaults

1800 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The "router lifetime" value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the security appliance as a default router on this interface.

Setting the value to a non-zero value to indicates that the security appliance should be considered a default router on this interface. The no-zero value for the "router lifetime" value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the security appliance should not be considered a default router on this interface.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

Syntax Description

value	The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default is 0.

Defaults

0 milliseconds.

Command Modes

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

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

Command History

Release	Modification
7.0	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 gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Defaults

Router advertisements are automatically sent on LAN interfaces if IPv6 unicast routing is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static entry from the neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

Syntax Description

if_name	The internal or external interface name designated by the **nameif** command.
ipv6_address	The IPv6 address that corresponds to the local data-link address.
mac_address	The local data-line (hardware MAC) address.

Defaults

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the **copy** command is used to store the configuration.

Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example adds a static entry for the an inside host with an IPv6 address of 3001:1::45A and a MAC address of 0002.7D1A.9472 to the neighbor discovery cache:

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

ipv6 route

To add an IPv6 route to the IPv6 routing table, use the **ipv6 route** command in global configuration mode. To remove an IPv6 default route, use the **no** form of this command.

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

Syntax Description

administrative-distance	(Optional) The administrative distance of the route. The default value is 1, which gives static routes precedence over any other type of routes except connected routes.
if_name	The name of the interface the route is being configured for.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network.
ipv6-prefix	The IPv6 network that is the destination of the static route. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Defaults

By default, the *administrative-distance* is 1.

Command Modes

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

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

Command History

Release	Modification
7.0	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:

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
hostname(config)# isakmp am-disable
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp disconnect-notify

To enable disconnect notification to peers, use the **isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

isakmp disconnect-notify

no isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance, use the **isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

isakmp enable *interface-name*

no isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
hostname(config)# no isakmp enable inside
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp identity

To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

no isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully-qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Defaults

The default ISAKMP identity is **isakmp identity hostname**.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPSec peer, depending on connection type:

```
hostname(config)# isakmp identity auto
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp ipsec-over-tcp

To enable IPSec over TCP, use the **isakmp ipsec-over-tcp** command in global configuration mode. To disable IPSec over TCP, use the **no** form of this command.

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPSec over TCP connections. You can list up to 10 ports. Port numbers can be in the range 1-65535. The default port number is 10000.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example, entered in global configuration mode, enables IPSec over TCP on port 45:

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp keepalive

To configure IKE DPD, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

isakmp keepalive [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

no isakmp keepalive disable

Syntax Description

disable	Disables IKE keepalive processing, which is enabled by default.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10 seconds for a LAN-to-LAN group, and 300 second for a remote access group.

Defaults

The default for a remote access group is a threshold of 300 seconds and a retry of 2 seconds.

For a LAN-to-LAN group, the default is a threshold of 10 seconds and a retry of 2 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0	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 nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **isakmp enable** command) in global configuration mode and then use the **isakmp nat-traversal** command. If you have enabled NAT traversal, you can disable it with the **no** form of this command.

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Defaults

By default, NAT traversal (**isakmp nat-traversal**) is disabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Network Address Translation (NAT), including Port Address Translation (PAT), is used in many networks where IPSec is also used, but there are a number of incompatibilities that prevent IPSec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The security appliance supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html, and NAT traversal is supported for both dynamic and static crypto maps.

This command enables NAT-T globally on the security appliance. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then enables NAT traversal with an interval of 30 seconds:

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy authentication

To specify an authentication method within an IKE policy, use the **isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting. DSA-Sig was added in 7.0.

Usage Guidelines

If you specify RSA signatures, you must configure the security appliance and its peer to obtain certificates from a certification authority (CA). If you specify preshared keys, you must separately configure these preshared keys within the security appliance and its peer.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy authentication** command. This example sets the authentication method of RSA Signatures to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is **des,** use the **no** form of this command.

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

Syntax Description

3des	Specifies that the Triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default ISAKMP policy encryption is **3des**.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
hostname(config)# isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 encryption 3des
```

```
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

isakmp policy *priority* **group** {**1** | **2** | **5** | **7**}

no isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
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:

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

Command History

Release	Modification
Preexisting	This command was preexisting. Group 7 was added.

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)# isakmp policy 40 group 2
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

isakmp policy *priority* **hash** {**md5** | **sha**}

no isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies that SHA-1 (HMAC variant) as the hash algorithm be used in the IKE policy.

Defaults

The default hash algorithm is SHA-1 (HMAC variant).

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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

priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for infinite lifetime.

Defaults

The default value is 86,400 seconds (one day).

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPSec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the security appliance sets up future IPSec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.
The following example, entered in global configuration mode, shows use of the **isakmp policy lifetime** command. This example sets the lifetime of the IKE security association to 50,400 seconds (14 hours) within the IKE policy with the priority number of 40.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
hostname(config)# isakmp policy 40 lifetime 0
```

Related Commands

clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the security appliance, use the **isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the security appliance, use the **no** form of this command.

isakmp reload-wait

no isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, tells the security appliance to wait until all active sessions have terminated before rebooting.

```
hostname(config)# isakmp reload-wait
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

issuer-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.
string	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		
				Multiple	
	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	•	•	•	•

Command History

Release	Modification
7.0	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.

join-failover-group

To assign a context to a failover group, use the **join-failover-group** command in context configuration mode. To restore the default setting, use the **no** form of this command.

join-failover-group *group_num*

no join-failover-group *group_num*

Syntax Description

group_num	Specifies the failover group number.

Defaults

Failover group 1.

Command Modes

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

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

Command History

Release	Modification
7.0	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

string	A case-sensitive, alphanumeric string, up to 64 characters long. Spaces are not permitted in the string. **Note** Kerberos realm names use numbers and upper-case letters only. Although the security appliance accepts lower-case letters in the *string* argument, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	Introduced in this release.

Usage Guidelines

This command is valid only for Kerberos servers.

The value of the *string* argument should match the output of the Microsoft Windows **set USERDNSDOMAIN** command when it is run on the Windows 2000 Active Directory server for the Kerberos realm. In the following example, EXAMPLE.COM is the Kerberos realm name:

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

The *string* argument must use numbers and upper-case letters only. The **kerberos-realm** command is case sensitive and the security appliance does not translate lower-case letters to upper-case letters.

Examples

The following sequence shows the **kerberos-realm** command to set the kerberos realm to "EXAMPLE.COM" in the context of configuring a AAA server host:

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration submode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Remove all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

key

To specify the server secret value used to authenticate the NAS to the AAA server, use the **key** command in aaa-server host mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove the key, use the **no** form of this command.The key (server secret) value authenticates the security appliance to the AAA server.

key *key*

no key

Syntax Description

key	An alphanumeric keyword, up to 127 characters long.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	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 PIX Firewall versions is automatically converted to the equivalent **key** command.

Examples

The following example configures a TACACS+ AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the key as “myexclusivemumblekey”.

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server configuration.

keypair

To specify the key pair whose public key is to be certified, use the **keypair** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

keypair *name*

no keypair

Syntax Description

name	Specify the name of the key pair.

Defaults

The default setting is not to include the key pair.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and specifies a key pair to be certified for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
crypto key generate dsa	Generates DSA keys.
crypto key generate rsa	Generates RSA keys.
default enrollment	Returns enrollment parameters to their defaults.

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		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **kill** command lets you terminate a Telnet session. Use the **who** command to see the Telnet session ID. When you kill a Telnet session, the security appliance lets any active commands terminate and then drops the connection without warning.

Examples

The following example shows how to terminate a Telnet session with the ID "2". First, the **who** command is entered to display the list of active Telnet sessions. Then the **kill 2** command is entered to terminate the Telnet session with the ID "2".

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

Related Commands

Command	Description
telnet	Configures Telnet access to the security appliance.
who	Displays a list of active Telnet sessions.

l2tp tunnel hello

To specify the interval between hello messages on L2TP over IPSec connections, use the **l2tp tunnel hello** command in global configuration mode. To remove the command from the configuration and set the default, use the no form of the command:

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

Syntax Description

interval	Interval between hello messages in seconds. The Default is 60 seconds. The range is 10 to 300 seconds.

Defaults

The default is 60 seconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **l2tp tunnel hello** command enables the security appliance to detect problems with the physical layer of the L2TP connection. The default is 60 secs. If you configure it to a lower value, connections that are experiencing problems are disconnected earlier.

Examples

The following example configures the interval between hello messages to 30 seconds:

```
hostname(config)# l2tp tunnel hello 30
```

Related Commands

Command	Description
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	Displays the details of L2TP connections.
vpn-tunnel-protocol l2tp-ipsec	Enables L2TP as a tunneling protocol for a specific tunnel group.

ldap-base-dn

To specify the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request, use the **ldap-base-dn** command in aaa-server host configuration mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, thus resetting the search to start at the top of the list, use the **no** form of this command.

ldap-base-dn *string*

no ldap-base-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request; for example, OU=Cisco. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

Start the search at the top of the list.

Command Modes

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

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

Command History

Release	Modification
7.0	Pre-existing command, modified for this release

Usage Guidelines

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP base DN as “starthere”.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-login-password	Specifies the password for the login DN.

ldap-defaults

To define LDAP default values, use the **ldap-defaults** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These default values are used only when the LDAP server requires them. To specify no LDAP defaults, use the **no** form of this command.

ldap-defaults *server* [*port*]

no ldap-defaults

Syntax Description

port	(Optional) Specifies the LDAP server port. If this parameter is not specified, the security appliance uses the standard LDAP port (389).
server	Specifies the IP address or domain name of the LDAP server. If one exists within the CRL distribution point, it overrides this value.

Defaults

The default setting is not set.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example defines LDAP default values on the default port (389):

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs

ldap-dn

To pass a X.500 distinguished name and password to an LDAP server that requires authentication for CRL retrieval, use the **ldap-dn** command in crl configure configuration mode. Crl configure configuration mode is accessible from crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

To specify no LDAP DN, use the **no** form of this command.

ldap-dn *x.500-name password*

no ldap-dn

Syntax Description

password	Defines a password for this distinguished name. The maximum field length is 128 characters.
x.500-name	Defines the directory path to access this CRL database, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum field length is 128 characters.

Defaults

The default setting is not on.

Command Modes

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

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

Command History

Release	Modification
7.0	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 accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command.

ldap-login-dn *string*

no ldap-login-dn

Syntax Description

string	A case-sensitive string of up to 128 characters that specifies the name of the directory object in the LDAP hierarchy. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Some LDAP servers, including the Microsoft Active Directory server, require that the security applianceestablish a handshake via authenticated binding before they will accept requests for any other LDAP operations. The security appliance identifies itself for authenticated binding by attaching a Login DN field to the user authentication request. The Login DN field describes the authentication characteristics of the security appliance. These characteristics should correspond to those of a user with administrator privileges.

For the *string* variable, enter the name of the directory object for VPN Concentrator authenticated binding, for example: cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com. For anonymous access, leave this field blank.

Examples

The following example configures an LDAP AAA server named “svrgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login DN as “myobjectname”.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
```

```
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host))# retry 7
hostname(config-aaa-server-host))# ldap-login-dn myobjectname
hostname(config-aaa-server-host))# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-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 accessibile from aaa-server protocol configuration mode. To remove this password specification, use the **no** form of this command:

ldap-login-password *string*

no ldap-login-password

Syntax Description

string	A case-sensitive, alphanumeric password, up to 64 characters long. The password cannot contain space characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is valid only for LDAP servers. The maximum password string length is 64 characters.

Examples

The following example configures an LDAP AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP login password as “obscurepassword”.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-base-dn	Specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request.
ldap-login-dn	Specifies the name of the directory object that the system should bind as.
ldap-naming-attribute	Specifies the Relative Distinguished Name attribute (or attributes) that uniquely identifies an entry on the LDAP server.
ldap-scope	Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request.

ldap-naming-attribute

To specify the Relative Distinguished Name attribute, use the **ldap-naming-attribute** command in aaa-server host mode. Aaa-server host configuration mode is accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-naming-attribute *string*

no ldap-naming-attribute

Syntax Description

string	The case-sensitive, alphanumeric Relative Distinguished Name attribute consisting of up to 128 characters, that uniquely identifies an entry on the LDAP server. Spaces are not permitted in the string, but other special characters are allowed.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Enter the Relative Distinguished Name attribute that uniquely identifies an entry on the LDAP server. Common naming attributes are Common Name (cn) and User ID (uid).

This command is valid only for LDAP servers. The maximum supported string length is 128 characters.

Examples

The following example configures an LDAP AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP naming attribute as “cn”.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)# exit
```

Related Commands

Command	Description
aaa-server host	Enters AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
ldap-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 accessibile from aaa-server protocol configuration mode. To remove this specification, use the **no** form of this command:

ldap-scope *scope*

no ldap-scope

Syntax Description

scope	The number of levels in the LDAP hierarchy for the server to search when it receives an authorization request. Valid values are: • **onelevel**—Search only one level beneath the Base DN • **subtree**—Search all levels beneath the Base DN

Defaults

The default value is **onelevel**.

Command Modes

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

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

Command History

Release	Modification
7.0	Pre-existing command, modified for this release

Usage Guidelines

Specifying the scope as **onelevel** results in a faster search, because only one level beneath the Base DN is searched. Specifying **subtree** is slower, because all levels beneath the Base DN are searched.

This command is valid only for LDAP servers.

Examples

The following example configures an LDAP AAA server named “svrgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures the LDAP scope to include the subtree levels.

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-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 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:

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

Command History

Release	Modification
7.0	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 *Cisco Security Appliance Command Line 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 security appliance before connecting.

log-adj-changes

To configure the router to send a syslog message when an OSPF neighbor goes up or down, use the **log-adj-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]

no log-adj-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **log-adj-changes** command is enabled by default; it appears in the running configuration unless removed with the **no** form of the command.

Examples

The following example disables the sending of a syslog message when an OSPF neighbor goes up or down:

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.

login

To log into privileged EXEC mode using the local user database (see the username command) or to change user names, use the **login** command in user EXEC mode.

login

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

From user EXEC mode, you can log in to privileged EXEC mode as any username in the local database using the **login** command. The **login** command is similar to the **enable** command when you have enable authentication turned on (see the **aaa authentication console** command). Unlike enable authentication, the **login** command can only use the local username database, and authentication is always required with this command. You can also change users using the **login** command from any CLI mode.

To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the **aaa authorization command** for more information.

Caution If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

Examples

The following example shows the prompt after you enter the **login** command:

```
hostname> login
```

```
Username:
```

Related Commands

Command	Description
aaa authorization command	Enables command authorization for CLI access.
aaa authentication console	Requires authentication for console, Telnet, HTTP, SSH, or **enable** command access.
logout	Logs out of the CLI.
username	Adds a user to the local database.

logging asdm

To send syslog messages to the ASDM log buffer, use the **logging asdm** command in global configuration mode. To disable logging to the ASDM log buffer, use the **no** form of this command.

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the ASDM log buffer. For information about creating lists, see the **logging list** command.

Defaults

ASDM logging is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Before any messages are sent to the ASDM log buffer, you must enable logging using the **logging enable** command.

When the ASDM log buffer is full, security appliance deletes the oldest message to make room in the buffer for new messages. To control the number of 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 log buffer enabled by the **logging buffered** command.

Examples

This example shows how enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages it contains.
logging asdm-buffer-size	Specifies the number of ASDM messages retained in the ASDM log buffer
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging configuration.

logging asdm-buffer-size

To specify the number of 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

num_of_msgs	Specifies the number of syslog messages that the security appliance retains in the ASDM log buffer.

Defaults

The default ASDM syslog buffer size is 100 messages.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When the ASDM log buffer is full, security appliance deletes the oldest message to make room in the buffer for new messages. To control whether logging to the ASDM log buffer is enabled or to control the kind of syslog messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

This example shows how enable logging and send to the ASDM log buffer messages of severity levels 0, 1, and 2. It also shows how to set the ASDM log buffer size to 200 messages.

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages it contains.
logging asdm	Enables logging to the ASDM log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffered

To enable the security appliance to send syslog messages to the log buffer, use the **logging buffered** command in global configuration mode. To disable logging to the log buffer, use the **no** form of this command.

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the log buffer. For information about creating lists, see the **logging list** command.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Buffer size is 4 KB.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the log buffer, you must enable logging using the **logging enable** command.

New messages append to the end of the buffer. When the buffer fills up, the security appliance clears it and continues adding messages to it. When the log buffer is full, security appliance deletes the oldest message to make room in the buffer for new messages. You can have buffer contents automatically saved each time the contents of the buffer have "wrapped", meaning that all the messages since the last save have been replaced by new messages. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

At any time, you can save the contents of the buffer to Flash memory. For more information, see the **logging savelog** command.

Syslog messages sent to the buffer can be viewed with the **show logging** command.

Examples

This example configures logging to the buffer for level 0 and level 1 events:

```
hostname(config)# logging buffered alerts
hostname(config)#
```

This example creates a list named notif-list with a maximum logging level of 7 and configures logging to the buffer for syslog messages identified by the notif-list list.

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.
logging list	Creates a reusable list of message selection criteria.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffer-size

To specify the size of the log buffer, use the **logging buffer-size** command in global configuration mode. To reset the log buffer to its default size of 4 KB of memory, use the **no** form of this command.

logging buffer-size *bytes*

no logging buffer-size *bytes*

Syntax Description

bytes	Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the security appliance uses 8 KB of memory for the log buffer.

Defaults

The log buffer size is 4 KB of memory.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

To see whether the security appliance is using a log buffer of a size other than the default buffer size, use the **show running-config logging** command. If the **logging buffer-size** command is not shown, then the security appliance uses a log buffer of 4 KB.

For more information about how the security appliance uses the buffer, see the **logging buffered** command.

Examples

This example enables logging, enables the logging buffer, and specifies that the security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging class

To configure for a message class the maximum logging level per logging destination, use the **logging class** command in global configuration mode. To remove a message class logging level configuration, use the **no** form of the command.

logging class *class destination level* [*destination level . . .*]

no logging class *class*

Syntax Description

class	Specifies the message class whose maximum logging levels per destination you are configuring. For valid values of class, see the "Usage Guidelines" section that follows.
destination	Specifies a logging destination for *class*. For the destination, the *level* determines the maximum logging level sent to *destination*. For valid values of *destination*, see the "Usage Guidelines" section that follows.
level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.

Defaults

By default, the security appliance does not apply logging levels on a logging destination and message class basis. Instead, each enabled logging destination receives messages for all classes at the logging level determined by the logging list or level specified when you enabled the logging destination.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Valid values for *class* include the following:

- **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

This example specifies that, for Failover-related messages, the maximum logging level for the ASDM log buffer is 2 and the maximum logging level for the system log buffer is 7:

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging console

To enable the security appliance to display 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 [*logging_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

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the console session. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not display syslog messages in console sessions by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the console, you must enable logging using the **logging enable** command.

Caution Using the **logging console** command could drastically degrade system performance. Instead, use the **logging buffered** command to start logging and 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 levels 0, 1, 2, and 3 to appears in console sessions:

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging debug-trace

To redirect debugging messages to logs as syslog message 711001 issued at severity level 7, use the **logging debug-trace** command in global configuration mode. To stop sending debugging messages to logs, use the **no** form of this command.

logging debug-trace

no logging debug-trace

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not include debug output in syslog messages.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Debug messages are generated as severity level 7 messages. They appear in logs with the syslog message number 711001, but do not appear in any monitoring session.

Examples

This example shows how enable logging, send log messages to the system log buffer, redirect debugging output to logs, and turn on debugging disk activity.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

An example of a debug message that could appear in the logs follows:

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging device-id

To configure the security appliance to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the use of a device ID, use the **no** form of this command.

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

Syntax Description

context-name	Use the name of the current context as the device ID.
hostname	Use the host name of the security appliance as the device ID.
ipaddress *interface_name*	Use as the device ID the IP address of the interface specified as *interface_name*. 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 security appliance uses to send the log data to the external server.
string *text*	Use as the device ID the characters contained in *text*, which can be up to 16 characters long. You cannot use white space characters or any of the following characters in *text*: • &—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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you use the **ipaddress** keyword, the device ID becomes the specified security appliance interface IP address, regardless of the interface from which the message is sent. This keyword provides a single, consistent device ID for all messages that are sent from the device.

Examples

This example shows how to configure a host named secappl-1:

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

In syslog messages, the host name secappl-1 appears at the beginning of messages, such as the following message:

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging emblem

To use the EMBLEM format for syslog messages sent to destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of EMBLEM format, use the **no** form of this command.

logging emblem

no logging emblem

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not use EMBLEM format for syslog messages.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed to be independent of the **logging host** command.

Usage Guidelines

The **logging emblem** command lets you to enable EMBLEM-format logging for all logging destinations other than syslog servers. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

Examples

This example shows how to enable logging and enable the use of EMBLEM-format for logging to all logging destinations except syslog servers:

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging enable

To enable logging for all configured output locations, use the **logging enable** command in global configuration mode. To disable logging, use the **no** form of this command.

logging enable

no logging enable

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from the **logging on** command.

Usage Guidelines

The **logging enable** command allows you to enable or disable sending syslog messages to any of the supported logging destinations. You can stop all logging with the **no logging enable** command.

You can enable logging to individual logging destinations with the following commands:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Examples

This example shows how to enable logging. The output of the **show logging** command illustrates how each possible logging destination must be enabled separately.

```
hostname(config)# logging enable
hostname(config)# show logging
Syslog logging: enabled
```

```
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Deny Conn when Queue Full: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging facility

To specify the logging facility used for messages sent to syslog servers, use the **logging facility** command in global configuration mode. To reset the logging facility to its default of 20, use the **no** form of this command.

logging facility *facility*

no logging facility

Syntax Description

facility	Specifies the syslog facility; valid values are 16 through 23.

Defaults

The default facility is 20 (LOCAL4).

Command Modes

The following table shows the modes in which you can enter the command, with the exceptions noted above in the Syntax Description section:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Syslog servers file messages based on the *facility* number in the message. There are eight possible facilities, 16 (LOCAL0) through 23 (LOCAL7).

Examples

This example shows how to specify that the security appliance specify the logging facility as 16 in syslog messages. The output of the **show logging** command includes the facility being used by the security appliance.

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
```

```
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging flash-bufferwrap

To enable the security appliance to write the log buffer to Flash memory every time the buffer is full of messages that have never been saved, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing of the log buffer to Flash memory, use the **no** form of this command.

logging flash-bufferwrap

no logging flash-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Writing the log buffer to Flash memory is disabled.
- Buffer size is 4 KB.
- Minimum free Flash memory is 3 MB.
- Maximum Flash memory allocation for buffer logging is 1 MB.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

For the security appliance to write the log buffer to Flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

While the security appliance writes log buffer contents to Flash memory, it continues storing to the log buffer continues any new event messages.

The security appliance creates log files with names that use a default time-stamp format, as follows:

`LOG-`*`YYYY-MM-DD-HHMMSS`*`.TXT`

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

The availability of Flash memory affects how the security appliance saves syslog messages using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

Examples

This example shows how enable logging, enable the log buffer, and enable the security appliance to write the log buffer to Flash memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all 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 log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging flash-maximum-allocation	Specifies the maximum amount of Flash memory that can be used for writing log buffer contents.
logging flash-minimum-free	Specifies the minimum amount of Flash memory that must be available for the security appliance to permit writing the log buffer to Flash memory.
show logging	Displays the enabled logging options.

logging flash-maximum-allocation

To specify the maximum amount of Flash memory that the security appliance uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. This command determines how much Flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands. To reset the maximum amount of Flash memory used for this purpose to its default size of 1 MB of Flash memory, use the **no** form of this command.

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

Syntax Description

kbytes	The largest amount of Flash memory, in kilobytes, that the security appliance can use to save log buffer data.

Defaults

The default maximum Flash memory allocation for log data is 1 MB.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** causes Flash memory use for log files to exceed the maximum amount specified by the **logging flash-maximum-allocation** command, the security appliance deletes the oldest log files to free sufficient memory for the new log file. If there are no files to delete or if, after all old files are deleted, free memory is too small for the new log file, the security appliance fails to save the new log file.

To see whether the security appliance has a maximum Flash memory allocation of a size different than the default size, use the **show running-config logging** command. If the **logging flash-maximum-allocation** command is not shown, then the security appliance uses a maximum of 1 MB for saved log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the security appliance uses the log buffer, see the **logging buffered** command.

Examples

This example shows how to enable logging, enable the log buffer, enable the security appliance to write the log buffer to Flash memory, with the maximum amount of Flash memory used for writing log files set to approximately 1.2 MB of memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging flash-minimum-free	Specifies the minimum amount of Flash memory that must be available for the security appliance to permit writing the log buffer to Flash memory.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging flash-minimum-free

To specify the minimum amount of free Flash memory that must exist before the security appliance saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. This command affects how much free Flash memory must exist before the security appliance saves log files created by the **logging savelog** and **logging flash-bufferwrap** commands. To reset the minimum required amount of free Flash memory to its default size of 3 MB, use the **no** form of this command.

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

Syntax Description

kbytes	The minimum amount of Flash memory, in kilobytes, that must be available before the security appliance saves a new log file.

Defaults

The default minimum free Flash memory is 3 MB.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The logging flash-minimum-free command specifies how much Flash memory the **logging savelog** and **logging flash-bufferwrap** commands must preserve at all times.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** would cause the amount of free Flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the security appliance fails to save the new log file.

Examples

This example shows how to enable logging, enable the log buffer, enable the security appliance to write the log buffer to Flash memory, and specify that the minimum amount of free Flash memory must be 4000 KB:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
```

```
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to Flash memory when the log buffer is full.
logging flash-maximum-allocation	Specifies the maximum amount of Flash memory that can be used for writing log buffer contents.
logging savelog	Saves the contents of the log buffer to Flash memory.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging from-address

To specify the sender email address for syslog messages emailed by the security appliance, use the **logging from-address** command in global configuration mode. All emailed syslog messages appear to come from the address you specify. To remove the sender email 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 email address, that is, the email address that syslog emails appear to come from. For example, cdb@example.com.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Sending syslog messages by email is enabled by the **logging mail** command.

The address specified with this command need not correspond to an existing email account.

Examples

To enable logging and set up the security appliance to send syslog messages by email, using the following 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.

you would enter the following commands:

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
```

```
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging mail	Enables the security appliance to send syslog messages by email and determines which messages are sent by email.
logging recipient-address	Specifies the email address to which emailed syslog messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging ftp-bufferwrap

To enable the security appliance to send the log buffer to an FTP server every time the buffer is full of messages that have never been saved, use the **logging ftp-bufferwrap** command in global configuration mode. To disable sending the log buffer to an FTP server, use the **no** form of this command.

logging ftp-bufferwrap

no logging ftp-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Sending the log buffer to an FTP server is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When you enable **logging ftp-bufferwrap**, the security appliance sends log buffer data to the FTP server you specify with the **logging ftp-server** command. While the security appliance sends log data to the FTP server, it continues storing to the log buffer continues any new event messages.

For the security appliance to send log buffer contents to an FTP server, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

The security appliance creates log files with names that use a default time-stamp format, as follows:

`LOG-`*`YYYY-MM-DD-HHMMSS`*`.TXT`

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Examples

This example shows how enable logging, enable the log buffer, specify an FTP server, and enable the security appliance to write the log buffer to an FTP server. This example specifies an FTP server whose host name is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the /syslogs directory.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-server	Specifies FTP server parameters for use with the **logging ftp-bufferwrap** command.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging ftp-server

To specify details about the FTP server the security appliance sends log buffer data to when **logging ftp-bufferwrap** is enabled, use the **logging ftp-server** command in global configuration mode. To remove all details about an FTP server, use the **no** form of this command.

logging ftp-server *ftp-server ftp_server path username password*

no logging ftp-server *ftp-server ftp_server path username password*

Syntax Description

ftp-server	External FTP server IP address or host name. **Note** If you specify a host name, be sure DNS is operating correctly on your network.
path	Directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. For example: `/security_appliances/syslogs/appliance107`
username	A username that is valid for logging into the FTP server.
password	The password for the username specified.

Defaults

No FTP server is specified by default.

Command Modes

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

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

Command History

Release	Modification
7.0	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 security appliance does not verify the FTP server information you specify. If you misconfigure any of the details, the security appliance fails to send log buffer data to the FTP server.

Examples

This example shows how enable logging, enable the log buffer, specify an FTP server, and enable the security appliance to write the log buffer to an FTP server. This example specifies an FTP server whose host name is logserver-352. The server can be accessed with the username logsupervisor and password 1luvMy10gs. Log files are to be stored in the /syslogs directory.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging history

To enable SNMP logging and specify which messages are to be sent to SNMP servers, use the **logging history** command in global configuration mode. To disable SNMP logging, use the **no** form of this command.

logging history [*logging_list* | *level*]

no logging history

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the SNMP server. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not log to SNMP servers by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging history** command allows you to enable logging to an SNMP server and to set the SNMP message level or event list.

Examples

This example shows how to enable SNMP logging and specify that messages of levels 0, 1, 2, and 3 are sent to the SNMP server configured:

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
snmp-server	Specifies SNMP server details.

logging host

To define a syslog server, use the **logging host** command in global configuration mode. To remove a syslog server definition, use the **no** form of this command.

logging host *interface_name syslog_ip* [**tcp/***port* | **udp/***port*] [**format emblem**]

logging host *interface_name syslog_ip*

Syntax Description

format emblem	(Optional) Enables EMBLEM format logging for the syslog server.
interface_name	Interface on which the syslog server resides.
syslog_ip	The IP address of the syslog server.
tcp	Specifies that the security appliance should use TCP to send messages to the syslog server.
udp	Specifies that the security appliance should use TCP to send messages to the syslog server.
port	The port that the syslog server listens to for messages. Valid port values are 1025 through 65535, for either protocol.

Defaults

The defaults are as follows:

- The default port numbers are as follows:
  - UDP port is 514
  - TCP port is 1470
- The default protocol is UDP.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging host** *ip_address* **format emblem** command allows you to 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 host, then the messages are sent to that host. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. However, a server can only be specified to receive either UDP or TCP, not both.

You can display only the *port* and *protocol* values that you previously entered by using the **show running-config logging** command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17. TCP ports work only with the security appliance syslog server. The *port* must be the same port on which the syslog server listens.

Examples

This example shows how to send syslog messages of levels 0, 1, 2, and 3 to a a syslog server that resides on the inside interface and uses the default protocol and port number.

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging list

To create a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs) use the **logging list** command in global configuration mode. To remove the list, use the **no** form of this command.

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

Syntax Description

class *event_class*	(Optional) Sets the class of events for syslog messages. For the level specified, only syslog messages of the class specified are identified by the command. See "Usage Guidelines" for a list of classes.
level *level*	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
message *start_id*[**-***end_id*]	Specified a message ID or range of IDs. To lookup the default level of a message, use the **show logging** command or see the *Cisco Security Appliance Logging Configuration and System Log Messages* guide.
name	Sets the logging list name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	Support for this command was introduced.

Usage Guidelines

Logging commands that can use lists are the following:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *event_class* include the following:

- **auth**—User authentication
- **bridge**—Transparent firewall
- **ca**—PKI certificate authority
- **config**—Command interface
- **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

Examples

This example shows how to use the logging list command:

```
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 preceding example states that syslog messages that match the criteria specified will be sent to the logging buffer. The criteria specified in this example are:

1. Syslog 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 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
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging mail

To enable the security appliance to send syslog messages by email and to determine which messages are sent by email, use the **logging mail** command in global configuration mode. To disable emailing syslog messages, use the **no** form of this command.

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the email recipient. For information about creating lists, see the **logging list** command.

Defaults

Logging to email is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Emailed syslog messages appear in the subject line of the emails sent.

Examples

To set up the security appliance to send syslog messages by email, using the following 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.

you would enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the email address from which emailed syslog messages appear to come.
logging list	Creates a reusable list of message selection criteria.
logging recipient-address	Specifies the email address to which emailed syslog messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging message

To specify the logging level of a 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 security appliance 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 security appliance 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 level for system log messages. For example, if you set the level to 3, then the security appliance generates system log 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.
syslog_id	The ID of the syslog message that you want to enable or disable or whose severity level you want to modify. To lookup the default level of a message, use the **show logging** command or see the *Cisco Security Appliance Logging Configuration and System Log Messages* guide.

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 control the severity level of a message.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

Examples

The series of commands in the following example illustrates the use of the **logging message** command to control both whether a message is enabled and the severity level of the messages

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

Command	Description
clear configure logging	Clears all logging configuration or message configuration only.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging monitor

To enable the security appliance to display 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

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the SSH or Telnet session. For information about creating lists, see the **logging list** command.

Defaults

The security appliance does not display syslog messages in SSH and Telnet sessions by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging monitor** command enables 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

This example shows how to enable the display of syslog messages in console sessions. The use of the **errors** keyword indicates that messages of 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 enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
terminal	Sets terminal line parameters.

logging permit-hostdown

To make the status of a TCP-based syslog server irrelevant to new user sessions, use the **logging permit-hostdown** command in global configuration mode. To cause the security appliance to deny new user sessions when a TCP-based syslog server is unavailable, use the **no** form of this command.

logging permit-hostdown

no logging permit-hostdown

Syntax Description

This command has no arguments or keywords.

Defaults

By default, if you have enabled logging to a syslog server that uses a TCP connection, the security appliance does not allow new network access sessions when the syslog server is unavailable for any reason.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If you are using TCP as the logging transport protocol for sending messages to a syslog server, the security appliance denies new network access sessions as a security measure if the security appliance is unable to reach the syslog server. You can use the **logging permit-hostdown** command to remove this restriction.

Examples

The following example makes the status of TCP-based syslog servers irrelevant to whether the security appliance permits new sessions. When the show running-config logging command includes in its output the show running-config logging command, the status of TCP-based syslog servers is irrelevant to new network access sessions.

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging queue

To specify how many syslog messages the security appliance may hold in its syslog queue prior to processing them according to logging configuration, use the **logging queue** command in global configuration mode. To reset the logging queue size to the default of 512 messages, use the **no** form of this command.

logging queue *queue_size*

no logging queue *queue_size*

Syntax Description

queue_size	The number of syslog messages permitted in the queue used for storing syslog messages prior to processing them. Valid values are from 0 to 8192 messages. Zero means that the queue is limited only by block memory availability.

Defaults

The default queue size is 512 messages.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When traffic is so heavy that the queue fills up, the security appliance may discard messages.

Examples

This example shows how to display the output of the **logging queue** and **show logging queue** commands:

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the **logging queue** command is set to 0, which means that the queue can hold as many messages as block memory availability allows. The syslog messages in the queue are processed by the security appliance in the manner dictated by logging configuration, such as sending syslog messages to mail recipients, saving them to Flash memory, and so forth.

The output of this example **show logging queue** command shows that 5 messages are queued, 3513 messages was the largest number of messages in the queue at one time since the security appliance was last booted, and that 1 message was discarded. Even though the queue was set for unlimited, the messages was discarded because no block memory was available to add the message to the queue.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging rate-limit

To limit the rate at which system log messages are generated, use the **logging rate-limit** command. To disable rate limiting, use the **no** form of this command.

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

unlimited	Disables rate limiting. This means that there is no limit on the logging rate.
num	Number of system messages that can be generated during the specified time interval. The valid range of values for *num* is 1 through 2147483647.
interval	(Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for *interval* is 1 through 2147483647.
message	Suppresses reporting of this system log message.
syslog_id	ID of the system log message to be suppressed. The valid range of values for *syslog_id* is 100000-999999.
level *severity_level*	Sets the severity level above which the security appliance suppresses messages. The valid range for *severity_level* is 1 through 7.

Defaults

The default setting for *interval* is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The system message severity levels are as follows:

- 0—System Unusable
- 1—Take Immediate Action
- 2—Critical Condition
- 3—Error Message
- 4—Warning Message

•5—Normal but significant condition

•6—Informational

•7—Debug Message

Examples

The following example shows how to limit the rate of system log message generation:

```
hostname(config)# logging rate-limit 5 message 106023
hostname(config)# logging rate-limit 10 60 level 7
```

Related Commands

Command	Description
clear configure logging rate-limit	Resets the logging rate-limit setting to its default.
show logging	Shows the messages currently in the internal buffer or to shows logging configuration settings
show running-config logging rate-limit	Shows the current logging rate-limit setting.

logging recipient-address

To specify the receiving email address for syslog messages emailed by the security appliance, use the **logging recipient-address** command in global configuration mode. To remove the receiving email address, use the **no** form of this command. You can configure up to 5 recipient addresses. If you want, each recipient address can have a different message level than that specified by the **logging mail** command.

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

Syntax Description

address	Specifies recipient email address when sending syslog messages by email.
level	Indicates that a logging level follows.
level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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. **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 level of 3, the security appliance sends all messages to the recipient, including those of levels 4, 5, 6, and 7.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Sending syslog messages by email is enabled by the **logging mail** command.

You can configure up to 5 **logging recipient-address** commands. Each command can have a different logging level than the others. This is useful when you want more urgent messages to go to a larger number of recipients than less urgent messages are sent to.

Examples

To set up the security appliance to send syslog messages by email, using the following 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.

you would enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the email address from which emailed syslog messages appear to come.
logging mail	Enables the security appliance to send syslog messages by email and determines which messages are sent by email.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging savelog

To save the log buffer to Flash memory, use the **logging savelog** command in privileged EXEC mode.

logging savelog [*savefile*]

Syntax Description

savefile	(Optional) Saved Flash memory file name. If you do not specify the file name, the security appliance, saves the file using a default time-stamp format, as follows: `LOG-YYYY-MM-DD-HHMMSS.TXT` where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Defaults

The defaults are as follows:

- Buffer size is 4 KB.
- Minimum free Flash memory is 3 MB.
- Maximum Flash memory allocation for buffer logging is 1 MB.
- The default log file name is described in the preceding table.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Before you can save the log buffer to Flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be saved to Flash memory. To enable logging to the buffer, use the **logging buffered** command.

Note The **logging savelog** command does not clear the buffer. To clear the buffer, use the **clear logging buffer** command.

Examples

This example enables logging and the log buffer, exits global configuration mode, and saves the log buffer to Flash memory, using the file name latest-logfile.txt:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all 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 log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.

logging standby

To enable the failover standby security appliance to send the syslog messages of this security appliance to logging destinations, use the **logging standby** command in global configuration mode. To disable syslog and SNMP logging, use the **no** form of this command.

logging standby

no logging standby

Syntax Description

This command has no arguments or keywords.

Defaults

The **logging standby** command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can enable **logging standby** to ensure that the syslog messages of the failover standby security appliance stay synchronized if failover occurs.

Note Using the **logging standby** command causes twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

Examples

The following example enables the security appliance to send syslog messages to the failover standby security appliance. The output of the **show logging** command reveals that this feature is enabled.

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
```

```
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
failover	Enables the failover feature.
logging enable	Enables logging.
logging host	Defines a syslog server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging timestamp

To specify that 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 security appliance 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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging timestamp** command makes the security appliance include a timestamp in all 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.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging trap

To specify which syslog messages the security appliance sends to a syslog server, use the **logging trap** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

logging trap [*logging_list* | *level*]

no logging trap

Syntax Description

level	Sets the maximum level for system log messages. For example, if you set the level to 3, then the security appliance generates system log messages for 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.
logging_list	Specifies the list that identifies the messages to send to the syslog server. For information about creating lists, see the **logging list** command.

Defaults

No default syslog trap is defined.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you are using TCP as the logging transport protocol, the security appliance denies new network access sessions as a security measure if the security appliance is unable to reach the syslog server, if the syslog server is misconfigured, or if the disk is full.

UDP-based logging does not prevent the security appliance from passing traffic if the syslog server fails.

Examples

This example shows how to send syslog messages of levels 0, 1, 2, and 3 to a a syslog server that resides on the inside interface and uses the default protocol and port number.

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

login-message

To create a message that prompts WebVPN users to log in, use the **login-message** command in webvpn mode. To remove a login message from the configuration and reset the default, use the **no** form of this command. To have no login message, use the **login-message** command without a string.

login-message [*string*]

no login-message

Syntax Description

string	(Optional) Specifies the HTML string for the login message. Maximum 255 characters. May contain 7-bit ASCII values and HTML tags and escape sequences.

Defaults

The default login message is "Please enter your username and password."

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to create the WebVPN message, "Welcome to Our Company. Please enter your username and password.":

```
hostname(config)# webvpn
hostname(config-webvpn)# login-message Welcome to Our Company. Please enter your username
and password.
```

logo

To specify a logo to display on the WebVPN login and home pages, use the **logo** command in webvpn mode. To remove a logo from the configuration and reset the default, use the **no** form of this command. To have no logo, use the **logo none** command. If the filename you specify does not exist, an error occurs. If you remove a logo file but the configuration still points to it, no logo displays.

logo {**file** *filename* | **none**}

no logo

Syntax Description

file *filename*	Specifies the filename for the logo image. Maximum length is 255 characters. File type must be JPG, PNG, or GIF, and must be less than 100 KB.
none	Indicates that there is no logo. Sets a null value, thereby disallowing a logo. Prevents inheriting a logo.

Defaults

The Cisco logo is the default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The administrator uploads this file to the security gateway. If you specify a file, and it does not exist, the security appliance generates an error.

Examples

The following example shows how to set a WebVPN logo with the filename MyCompanylogo.gif:

```
hostname(config)# webvpn
hostname(config-webvpn)# logo MyCompanylogo.gif
```

logout

To exit from the CLI, use the **logout** command in user EXEC mode.

logout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logout** command lets you log out of the security appliance. You can use the **exit** or **quit** commands to go back to unprivileged mode.

Examples

The following example shows how to log out of the security appliance:

```
hostname> logout
```

Related Commands

Command	Description
login	Initiates the log-in prompt.
exit	Exits an access mode.
quit	Exits configuration or privileged mode.

logout-message

To create a logout message that WebVPN presents to users logging out, use the **logout-message** command in webvpn mode. To remove a logout message from the configuration and reset the default, use the **no** form of this command. To have no logout message, use the **logout-message** command without a string.

logout-message [*string*]

no logout-message

Syntax Description

string	(Optional) Specifies the HTML string for the logout message. Maximum 255 characters. May contain 7-bit ASCII values and HTML tags and escape sequences.

Defaults

The default logout message is "Goodbye."

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to create the WebVPN logout message, "Farewell! Be careful crossing the street!":

```
hostname(config)# logout-message Farewell! Be careful crossing the street!
```