CHAPTER 22

packet-tracer through pwd Commands

packet-tracer

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

packet-tracer input [*src_int*] *protocol src_addr src_port dest_addr dest_port* [**detailed**] [**xml**]

no packet-tracer

Syntax Description

input *src_int*	Specifies the source interface for the packet trace.
protocol	Specifies the protocol type for the packet trace. Available protocol type keywords are *icmp*, *rawip*, *tcp* or *udp*.
src_addr	Specifies the source address for the packet trace.
src_port	Specifies the source port for the packet trace.
dest_addr	Specifies the destination address for the packet trace.
dest_port	Specifies the destination port for the packet trace.
detailed	(Optional) Provides detailed packet trace information.
xml	(Optional) Displays the trace capture in XML format.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In addition to capturing packets, it is possible to trace the lifespan of a packet through the security appliance to see if it is behaving as expected. The **packet-tracer** command lets you do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines which caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

The **packet-tracer** command provides detailed information about the packets and how they are processed by the security appliance. In the instance that a command from the configuration did not cause the packet to drop, the **packet-tracer** command will provide information about the cause in an easily readable manner. For example if a packet was dropped because of an invalid header validation, a message is displayed that says, "packet dropped due to bad ip header (reason)."

Note The **packet-tracer** command can generate packets based on the 5 tuple information—source IP, destination IP, source port, destination port, and protocol. The packet tracer does not populate the data part of the packet and as a result some engine checks will not be applicable. The packet tracer will show that the packet is dropped not because it did not pass the inspection checks but because there is not enough data to test against the inspection checks. For example the packet tracer will show drops incorrectly for dns traffic if the dns inspection is enabled.

Examples

To enable packet tracing from inside host 10.2.25.3 to external host 209.165.202.158 with detailed information, enter the following:

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

Related Commands

Command	Description
capture	Captures packet information, including trace packets.
show capture	Displays the capture configuration when no options are specified.

page style

To customize the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **page style** command in webvpn customization mode:

page style *value*

[**no**] **page style** *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

value	Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default page style is background-color:white;font-family:Arial,Helv,sans-serif

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the page style to large:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
title	Customizes the title of the WebVPN page

pager

To set the default number of lines on a page before the "---more---" prompt appears for Telnet sessions, use the **pager** command in global configuration mode.

pager [lines] *lines*

Syntax Description

[**lines**] *lines*	Sets the number of lines on a page before the "---more---" prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Defaults

The default is 24 lines.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from a privileged EXEC mode command to a global configuration mode command. The **terminal pager** command was added as the privileged EXEC mode command.

Usage Guidelines

This command changes the default pager line setting for Telnet sessions. If you want to temporarily change the setting only for the current session, use the **terminal pager** command.

If you Telnet to the admin context, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

Examples

The following example changes the number of lines displayed to 20:

```
hostname(config)# pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messsages to display on the Telnet session.
terminal pager	Sets the number of lines to display in a Telnet session before the "`---more---`" prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

parameters

To enter parameters configuration mode to set parameters for an inspection policy map, use the **parameters** command in policy-map configuration mode.

parameters

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

An inspection policy map may support one or more **parameters** commands. Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

Examples

The following example shows how to set the maximum message length for DNS packets in the default inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

participate

To force the device to participate in the virtual load-balancing cluster, use the **participate** command in VPN load-balancing mode. To remove a device from participation in the cluster, use the **no** form of this command.

participate

no participate

Syntax Description

This command has no arguments or keywords.

Defaults

The default behavior is that the device does not participate in the vpn load-balancing cluster.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first configure the interface using the **interface** and **nameif** commands, and use the **vpn load-balancing** command to enter VPN load-balancing mode. You must also have previously configured the cluster IP address using the **cluster ip** command and configured the interface to which the virtual cluster IP address refers.

This command forces this device to participate in the virtual load-balancing cluster. You must explicitly issue this command to enable participation for a device.

All devices that participate in a cluster must share the same cluster-specific values: ip address, encryption settings, encryption key, and port.

Note When using encryption, you must have previously configured the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If isakmp is not enabled on the load-balancing inside interface, you get an error message when you try to configure cluster encryption.

If isakmp was enabled when you configured the **cluster encryption** command, but was disabled before you configured the **participate** command, you get an error message when you enter the **participate** command, and the local device will not participate in the cluster.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **participate** command that enables the current device to participate in the vpn load-balancing cluster:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

Related Commands

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

passive-interface

To disable the transmission of RIP routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable RIP routing updates on an interface, use the **no** form of this command.

passive-interface [**default** | *if_name*]

no passive-interface {**default** | *if_name*}

Syntax Description

default	(Optional) Set all interfaces to passive mode.
if_name	(Optional) The interface on which RIP is set to passive mode.

Defaults

All interfaces are enabled for active RIP when RIP is enabled.

If an interface or the **default** keyword is not specified, the commands defaults to **default** and appears in the configuration as `passive-interface default`.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables but does not broadcast routing updates.

Examples

The following example sets the outside interface to passive RIP. The other interfaces on the security appliance send and receive RIP updates.

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.

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

passwd

To set the login password, use the **passwd** command in global configuration mode. To set the password back to the default of "cisco," use the **no** form of this command. You are prompted for the login password when you access the CLI as the default user using Telnet or SSH. After you enter the login password, you are in user EXEC mode.

{**passwd** | **password**} *password* [**encrypted**]

no {**passwd** | **password**} *password*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **passwd** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config passwd** command.
passwd | **password**	You can enter either command; they are aliased to each other.
password	Sets the password as a case-sensitive string of up to 80 characters. The password must not contains spaces.

Defaults

The default password is "cisco."

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

This login password is for the default user. If you configure CLI authentication per user for Telnet or SSH using the **aaa authentication console** command, then this password is not used.

Examples

The following example sets the password to Pa$$w0rd:

```
hostname(config)# passwd Pa$$w0rd
```

The following example sets the password to an encrypted password that you copied from another security appliance:

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

password (crypto ca trustpoint)

To specify a challenge phrase that is registered with the CA during enrollment, use the **password** command in crypto ca trustpoint configuration mode. The CA typically uses this phrase to authenticate a subsequent revocation request. To restore the default setting, use the **no** form of the command.

password *string*

no password

Syntax Description

string	Specifies the name of the password as a character string. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, "hello 21" is a legal password, but "21 hello" is not. The password checking is case sensitive. For example, the password "Secret" is different from the password "secret".

Defaults

The default setting is to not include a password.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command lets you specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the security appliance.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes a challenge phrase registered with the CA in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
hostname(ca-trustpoint)#
```

Related Commands

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

password-management

To enable password management, use the **password-management** command in tunnel-group general-attributes configuration mode. To disable password management, use the **no** form of this command. To reset the number of days to the default value, use the **no** form of the command with the **password-expire-in-days** keyword specified.

password-management [**password-expire-in-days** *days*]

no password-management

no password-management password-expire-in-days [*days*]

Syntax Description

days	Specifies the number of days (0 through 180) before the current password expires. This parameter is required if you specify the **password-expire-in-days** keyword.
password-expire-in-days	(Optional) Indicates that the immediately following parameter specifies the number of days before the current password expires that the security appliance starts warning the user about the pending expiration. This option is valid only for LDAP servers.

Defaults

If you do not specify this command, no password management occurs. If you do not specify the **password-expire-in-days** keyword, the default length of time to start warning before the current password expires is 14 days.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

You can configure this attribute for IPSec remote access and WebVPN tunnel-groups.

When you configure this command, the security appliance notifies the remote user at login that the user's current password is about to expire or has expired. The security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. This command is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

Note that this does not change the number of days before the password expires, but rather, the number of days ahead of expiration that the security appliance starts warning the user that the password is about to expire.

If you do specify the **password-expire-in-days** keyword, you must also specify the number of days.

Specifying this command with the number of days set to 0 disables this command. The security appliance does not notify the user of the pending expiration, but the user can change the password after it expires.

Examples

The following example sets the days before password expiration to begin warning the user of the pending expiration to 90 for the WebVPN tunnel group "testgroup":

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

The following example uses the default value of 14 days before password expiration to begin warning the user of the pending expiration for the IPSec remote access tunnel group "QAgroup":

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
passwd	Sets the login password.
radius-with-expiry	Enables negotiation of password update during RADIUS authentication (Deprecated).
show running-config passwd	Shows the login password in encrypted form.
tunnel-group general-attributes	Configures the tunnel-group general-attributes values.

password-parameter

To specify the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication, use the **password-parameter** command in aaa-server- host configuration mode. This is an SSO with HTTP Forms command.

password-parameter *string*

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

Syntax Description

string	The name of the password parameter included in the HTTP POST request. The maximum password length is 128 characters.

Defaults

There is no default value or behavior.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The required command **password-parameter** specifies that the POST request must include a user password parameter for SSO authentication.

Note At login, the user enters the actual password value which is entered into the POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies a password parameter named user_password:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
hostname(config-aaa-server-host)#
```

Related Commands

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

password-prompt

To customize the password prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **password-prompt** command from webvpn customization mode:

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default text of the password prompt is "PASSWORD:".

The default style of the password prompt is color:black;font-weight:bold;text-align:right.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Password:", and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# password-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# password-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page
username-prompt	Customizes the username prompt of the WebVPN page

password-storage

To let users store their login passwords on the client system, use the **password-storage enable** command in group-policy configuration mode or username configuration mode. To disable password storage, use the **password-storage disable** command.

To remove the password-storage attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for password-storage from another group policy.

password-storage {enable | disable}

no password-storage

Syntax Description

disable	Disables password storage.
enable	Enables password storage.

Defaults

Password storage is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enable password storage only on systems that you know to be in secure sites.

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

Examples

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

To specify whether to validate the identity of the peer using the peer's certificate, use the **peer-id-validate** command in tunnel-group ipsec-attributes mode. To return to the default value, use the **no** form of this command.

peer-id-validate *option*

no peer-id-validate

Syntax Description

option	Specifies one of the following options: • **req**: required • **cert**: if supported by certificate • **nocheck**: do not check

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0.1	This command was introduced.

Usage Guidelines

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

Examples

The following example entered in config-ipsec configuration mode, requires validating the peer using the identity of the peer's certificate for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

perfmon

To display performance information, use the **perfmon** command in privileged EXEC mode.

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

Syntax Description

verbose	Displays performance monitor information at the security appliance console.
interval *seconds*	Specifies the number of seconds before the performance display is refreshed on the console.
quiet	Disables the performance monitor displays.
settings	Displays the interval and whether it is quiet or verbose.
detail	Displays detailed information about performance.

Defaults

The *seconds* is 120 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the security appliance.
7.2(1)	Support for the **detail** keyword was added.

Usage Guidelines

The **perfmon** command allows you to monitor the performance of the security appliance. Use the **show perfmon** command to display the information immediately. Use the **perfmon verbose** command to display the information every 2 minutes continuously. Use the **perfmon interval** *seconds* command with the **perfmon verbose** command to display the information continuously every number of seconds that you specify.

An example of the performance information is displayed as follows:

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s

FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

This information lists the number of translations, connections, Websense requests, address translations (called “fixups”), and AAA transactions that occur each second.

Examples

This example shows how to display the performance monitor statistics every 30 seconds on the security appliance console:

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

Command	Description
show perfmon	Displays performance information.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To disable, use the **no** form of this command.

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

Syntax Description

days-of-the-week	(Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the **to** keyword is required to complete the range "from start-time to end-time."

Defaults

If a value is not entered with the **periodic** command, access to the security appliance as defined with the **time-range** command is in effect immediately and always on.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the security appliance; however, the feature works best with NTP synchronization.

Examples

Some examples follow:

If you want:	Enter this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	**periodic weekdays 8:00 to 18:00**
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	**periodic daily 8:00 to 18:00**
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	**periodic monday 8:00 to friday 20:00**
All weekend, from Saturday morning through Sunday night	**periodic weekend 00:00 to 23:59**
Saturdays and Sundays, from noon to midnight	**periodic weekend 12:00 to 23:59**

The following example shows how to allow access to the security appliance on Monday through Friday, 8:00 a.m. to 6:00 p.m. only:

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

The following example shows how to allow access to the security appliance on specific days (Monday, Tuesday, and Friday), 10:30 a.m. to 12:30 p.m.:

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the security appliance.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
time-range	Defines access control to the security appliance based on time.

permit errors

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, use the **permit errors** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to remove the command.

permit errors

no permit errors

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all invalid packets or packets that failed, during parsing, are dropped.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **permit errors** command in GTP map configuration mode to allow any packets that are invalid or encountered an error during inspection of the message to be sent through the security appliance instead of being dropped.

Examples

The following example permits traffic containing invalid packets or packets that failed, during parsing:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
hostname(config-gtpmap)#
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.

Commands	Description
permit response	Supports load-balancing GSNs.
show service-policy inspect gtp	Displays the GTP configuration.

permit response

To support load-balancing GSNs, use the **permit response** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. The permit response command supports load-balancing GSNs by allowing GTP responses from a different GSN than the response was sent to. Use the **no** form of this command to remove the command.

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

Syntax Description

from-object-group *from_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can send responses to the set of GSNs in the object-group specified by the *to_obj_group_id* argument. The security appliance supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.
to-object-group *to_obj_group_id*	Specifies the name of the object-group configured with the **object-group** command which can receive responses from the set of GSNs in the object-group specified by the *from_obj_group_id* argument. The security appliance supports only object-groups containing network-objects with IPv4 addresses. IPv6 addresses are currently not supported with GTP.

Defaults

By default, the security appliance drops GTP responses from GSNs other than the host to which the request was sent.

Command Modes

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

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

Command History

Release	Modification
7.0(1)(4)	This command was introduced.

Usage Guidelines

Use the **permit response** command in GTP map configuration mode to support load-balancing GSNs. The **permit response** command configures the GTP map to allow GTP responses from a different GSN than the response was sent to.

You identify the pool of load-balancing GSNs as a network object. Likewise, you identify the SGSN as a network object. If the GSN responding belongs to the same object group as the GSN that the GTP request was sent to and if the SGSN is in a object group that the responding GSN is permitted to send a GTP response to, the security appliance permits the response.

Examples

The following example permits GTP responses from any host on the 192.168.32.0 network to the host with the IP address 192.168.112.57:

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
permit errors	Allow invalid GTP packets.
show service-policy inspect gtp	Displays the GTP configuration.

pfs

To enable PFS, use the **pfs enable** command in group-policy configuration mode. To disable PFS, use the **pfs disable** command. To remove the PFS attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for PFS from another group policy.

In IPSec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.

pfs {enable | disable}

no pfs

Syntax Description

disable	Disables PFS.
enable	Enables PFS.

Defaults

PFS is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The PFS setting on the VPN Client and the security appliance must match.

Examples

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

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

pim

To re-enable PIM on an interface, use the **pim** command in interface configuration mode. To disable PIM, use the **no** form of this command.

pim

no pim

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM on all interfaces by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **multicast-routing** command enables PIM on all interfaces by default. Only the **no** form of the **pim** command is saved in the configuration.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

Examples

The following example disables PIM on the selected interface:

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

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim accept-register

To configure the security appliance to filter PIM register messages, use the **pim accept-register** command in global configuration mode. To remove the filtering, use the **no** form of this command.

pim accept-register {**list** *acl* | **route-map** *map-name*}

no pim accept-register

Syntax Description

list *acl*	Specifies an access list name or number. Use only standard host ACLs with this command; extended ACLs are not supported.
route-map *map-name*	Specifies a route-map name. Use standard host ACLs in the referenced route-map; extended ACLs are not supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the security appliance will immediately send back a register-stop message.

Examples

The following example restricts PIM register messages to those from sources defined in the access list named “no-ssm-range”:

```
hostname(config)# pim accept-register list no-ssm-range
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim bidir-neighbor-filter

To control which bidir-capable neighbors can participate in the DF election, use the **pim bidir-neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. The access list defines the neighbors that can participate in bidir DF elections. Use only standard ACLs with this command; extended ACLs are not supported.

Defaults

All routers are considered to be bidir capable.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled for bidir to elect a DF.

The **pim bidir-neighbor-filter** command enables the transition from a sparse-mode-only network to a bidir network by letting you specify the routers that should participate in DF election while still allowing all routers to participate in the sparse-mode domain. The bidir-enabled routers can elect a DF from among themselves, even when there are non-bidir routers on the segment. Multicast boundaries on the non-bidir routers prevent PIM messages and data from the bidir groups from leaking in or out of the bidir subset cloud.

When the **pim bidir-neighbor-filter** command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election does not occur.
- If a denied neighbor supports bidir, then DF election does not occur.
- If a denied neighbor does not support bidir, the DF election can occur.

Examples

The following example allows 10.1.1.1 to become a PIM bidir neighbor:

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

Related Commands

Command	Description
multicast boundary	Defines a multicast boundary for administratively-scoped multicast addresses.
multicast-routing	Enables multicast routing on the security appliance.

pim dr-priority

To configure the neighbor priority on the security appliance used for designated router election, use the **pim dr-priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

pim dr-priority *number*

no pim dr-priority

Syntax Description

number	A number from 0 to 4294967294. This number is used to determine the priority of the device when determining the designated router. Specifying 0 prevents the security appliance from becoming the designated router.

Defaults

The default value is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The device with the largest priority value on an interface becomes the PIM designated router. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the DR. If a device does not include the DR-Priority Option in hello messages, it is regarded as the highest-priority device and becomes the designated router. If multiple devices do not include this option in their hello messages, then the device with the highest IP address becomes the designated router.

Examples

The following example sets the DR priority for the interface to 5:

```
hostname(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim hello-interval

To configure the frequency of the PIM hello messages, use the **pim hello-interval** command in interface configuration mode. To restore the hello-interval to the default value, use the **no** form of this command.

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the security appliance waits before sending a hello message. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.

Defaults

30 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the PIM hello interval to 1 minute:

```
hostname(config-if)# pim hello-interval 60
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim join-prune-interval

To configure the PIM join/prune interval, use the **pim join-prune-interval** command in interface configuration mode. To restore the interval to the default value, use the **no** form of this command.

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

Syntax Description

seconds	The number of seconds that the security appliance waits before sending a join/prune message. Valid values range from 10 to 600 seconds. 60 seconds is the default.

Defaults

60 seconds

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example sets the PIM join/prune interval to 2 minutes:

```
hostname(config-if)# pim join-prune-interval 120
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim neighbor-filter

To control which neighbor routers can participate in PIM, use the **pim neighbor-filter** command in interface configuration mode. To remove the filtering, use the **no** form of this command.

pim neighbor-filter *acl*

no pim neighbor-filter *acl*

Syntax Description

acl	Specifies an access list name or number. Use only standard ACLs with this command; extended ACLs are not supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command defines which neighbor routers can participate in PIM. If this command is not present in the configuration then there are no restrictions.

Multicast routing and PIM must be enabled for this command to appear in the configuration. If you disable multicast routing, this command is removed from the configuration.

Examples

The following example prevents the router with the IP address 10.1.1.1 from becoming a PIM neighbor on interface GigabitEthernet0/2:

```
hostname(config)# access-list pim_filter deny 10.1.1.1 255.255.255.255
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim old-register-checksum

To allow backward compatibility on a rendezvous point (RP) that uses old register checksum methodology, use the **pim old-register-checksum** command in global configuration mode. To generate PIM RFC-compliant registers, use the **no** form of this command.

pim old-register-checksum

no pim old-register-checksum

Syntax Description

This command has no arguments or keywords.

Defaults

The security appliance generates PIM RFC-compliant registers.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance software accepts register messages with checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS method—accepting register messages with the entire PIM message for all PIM message types. The **pim old-register-checksum** command generates registers compatible with Cisco IOS software.

Examples

The following example configures the security appliance to use the old checksum calculations:

```
hostname(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

pim rp-address

To configure the address of a PIM rendezvous point (RP), use the **pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

pim rp-address *ip_address* [*acl*] [**bidir**]

no pim rp-address *ip_address*

Syntax Description

acl	(Optional) The name or number of a standard access list that defines which multicast groups the RP should be used with. Do not use a host ACL with this command.
bidir	(Optional) Indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM sparse mode.
ip_address	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.

This command has no arguments or keywords.

Defaults

No PIM RP addresses are configured.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain require knowledge of the well-known PIM RP address. The address is statically configured using this command.

Note The security appliance does not support Auto-RP; you must use the **pim rp-address** command to specify the RP address.

You can configure a single RP to serve more than one group. The group range specified in the access list determines the PIM RP group mapping. If the an access list is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

Note The security appliance always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Examples

The following example sets the PIM RP address to 10.0.0.1 for all multicast groups:

```
hostname(config)# pim rp-address 10.0.0.1
```

Related Commands

Command	Description
pim accept-register	Configures candidate RPs to filter PIM register messages.

pim spt-threshold infinity

To change the behavior of the last hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

pim spt-threshold infinity [**group-list** *acl*]

no pim spt-threshold

Syntax Description

group-list *acl*	(Optional) Indicates the source groups restricted by the access list. The *acl* argument must specify a standard ACL; extended ACLs are not supported.

Defaults

The last hop PIM router switches to the shortest-path source tree by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If the **group-list** keyword is not used, this command applies to all multicast groups.

Examples

The following example causes the last hop PIM router to always use the shared tree instead of switching to the shortest-path source tree:

```
hostname(config)# pim spt-threshold infinity
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

ping

To determine if other IP addresses are visible from the security appliance, use the **ping** command in privileged EXEC mode.

ping [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

Syntax Description

data *pattern*	(Optional) Specifies the 16-bit data pattern in hexidecimal.
host	Specifies the IPv4 or IPv6 address or name of the host to ping. The name can be a DNS name or a name assigned with the **name** command. The maximum number of characters for DNA names is 128, and the maximum number of characters for names created with the **name** command is 63.
if_name	(Optional) Specifies the interface name, as configured by the **nameif** command, by which the *host* is accessible. If not supplied, then the *host* is resolved to an IP address and then the routing table is consulted to determine the destination interface.
repeat *count*	(Optional) Specifies the number of times to repeat the ping request.
size *bytes*	(Optional) Specifies the datagram size in bytes.
timeout *seconds*	(Optional) Specifies the the number of seconds to wait before timing out the ping request.
validate	(Optional) Specifies to validate reply data.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	Support for DNS names added.

Usage Guidelines

The **ping** command allows you to determine if the security appliance has connectivity or if a host is available on the network. If the security appliance has connectivity, ensure that the **icmp permit any** *interface* command is configured. This configuration is required to allow the security appliance to respond and accept messages generated from the **ping** command. The **ping** command output shows if the response was received. If a host is not responding, when you enter the **ping** command, a message similar to the following displays:

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Use the **show interface** command to ensure that the security appliance is connected to the network and is passing traffic. The address of the specified *if_name* is used as the source address of the ping.

If you want internal hosts to ping external hosts, you must do one of the following:

- Create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list acl_grp permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.
- Configure the ICMP inspection engine using the **inspect icmp** command. For example, adding the **inspect icmp** command to the **class default_inspection** class for the global service policy allows echo replies through the security appliance for echo requests initiated by internal hosts.

You can also perform an extended ping, which allows you to enter the keywords one line at a time.

If you are pinging through the security appliance between hosts or routers, but the pings are not successful, use the **capture** command to monitor the success of the ping.

The security appliance **ping** command does not require an interface name. If you do not specify an interface name, the security appliance checks the routing table to find the address that you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

Examples

The following example shows how to determine if other IP addresses are visible from the security appliance:

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following example specifies a host using a DNS name:

```
hostname# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following is an example of an extended ping:

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Related Commands

Command	Description
capture	Captures packets at an interface
icmp	Configures access rules for ICMP traffic that terminates at an interface.
show interface	Displays information about the VLAN configuration.

police

To apply QoS policing to a class map, use the **police** command in class configuration mode. To remove the rate-limiting requirement, use the **no** form of this command. Policing is a way of ensuring that no traffic exceeds the maximum rate (in bits/second) that you configure, thus ensuring that no one traffic flow can take over the entire resource. When traffic exceeds the maximum rate, the security appliance drops the excess traffic. Policing also sets the largest single burst of traffic allowed.

police {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

no police

Syntax Description

conform-burst	Specifies the maximum number of instantaneous bytes allowed in a sustained burst before throttling to the conforming rate value, between 1000 and 512000000 bytes.
conform-action	Sets the action to take when the rate is less than the *conform_burst* value.
conform-rate	Sets the rate limit for this traffic flow; between 8000 and 2000000000 bits per second.
drop	Drops the packet.
exceed-action	Sets the action to take when the rate is between the *conform-rate* value and the *conform-burst* value.
input	Enables policing of traffic flowing in the input direction.
output	Enables policing of traffic flowing in the output direction.
transmit	Transmits the packet.

Defaults

No default behavior or variables.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Added the **input** option. Policing traffic in the inbound direction is now supported.

Usage Guidelines

To enable policing, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform policing.

2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **police**—Enable policing for the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

Note The **police** command merely enforces the maximum speed and burst rate, forcing them to the conforming rate value. It does not enforce the **conform-action** or the **exceed-action** specification if these are present.

Note When the conform-burst parameter is omitted, the default value is assumed to be 1/32 of the conform-rate in bytes (that is, with a conform rate of 100,000, the default conform-burst value would be 100,000/32 = 3,125). Note that the conform-rate is in bits/second, whereas the conform-burst is in bytes.

You can configure each of the QoS features alone if desired for the security appliance. Often, though, you configure multiple QoS features on the security appliance, so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).

  You cannot configure priority queueing and policing for the same set of traffic.
- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the security appliance does not restrict you from configuring this.

If a service policy is applied or removed from an interface that has existing VPN client/LAN-to-LAN or non-tunneled traffic already established, the QoS policy is not applied or removed from the traffic stream. To apply or remove the QoS policy for such connections, you must clear (that is, drop) the connections and re-establish them.

Examples

The following is an example of a **police** command for the output direction that sets the conform rate to 100,000 bits per second, a burst value of 20,000 bytes, and specifies that traffic that exceeds the burst rate will be dropped:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class-map firstclass
hostname(config-cmap)# class localclass
hostname(config-pmap-c)# police output 100000 20000 exceed-action drop
hostname(config-cmap-c)# class class-default
hostname(config-pmap-c)#
```

The following example shows how to do rate-limiting on traffic destined to an internal web server.

```
hostname# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
hostname# class-map http_traffic
hostname(config-cmap)# match access-list http_traffic
hostname(config-cmap)# policy-map outside_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# police input 56000
hostname(config-pmap-c)# service-policy outside_policy interface outside
hostname(config)#
```

Related Commands

class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

policy

To specify the source for retrieving the CRL, use the **policy** command in ca-crl configuration mode.

policy {**static | cdp | both**}

Syntax Description

both	Specifies that if obtaining a CRL using the CRL distribution point fails, retry using static CDPs up to a limit of five.
cdp	Uses the CDP extension embedded within the certificate being checked. In this case, the security appliance retrieves up to five CRL distributions points from the CDP extension of the certificate being verified and augments their information with the configured default values, if necessary. If the security appliance attempt to retrieve a CRL using the primary CDP fails, it retries using the next available CDP in the list. This continues until either the security appliance retrieves a CRL or exhausts the list.
static	Uses up to five static CRL distribution points. If you specify this option, specify also the LDAP or HTTP URLs with the **protocol** command.

Defaults

The default setting is **cdp**.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and configures CRL retrieval to occur using the CRL distribution point extension in the certificate being checked or if that fails, to use static CDPs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
url	Creates and maintains a list of static URLs for retrieving CRLs.

policy-map

When using the Modular Policy Framework, assign actions to traffic that you identified with a Layer 3/4 class map (the **class-map** or **class-map type management** command) by using the **policy-map** command (without the **type** keyword) in global configuration mode. To remove a Layer 3/4 policy map, use the **no** form of this command.

policy-map *name*

no policy-map *name*

Syntax Description

name	Specifies the name for this policy map up to 40 characters in length. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Defaults

By default, the configuration includes a policy that matches all default application inspection traffic and applies certain inspections to the traffic on all interfaces (a global policy). Not all inspections are enabled by default. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one. (An interface policy overrides the global policy for a particular feature.)

The default policy includes the following application inspections:

- DNS inspection for the maximum message length of 512 bytes
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

The default policy configuration includes the following commands:

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
    message-length maximum 512
policy-map global_policy
```

```
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
service-policy global_policy global
```

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** or **class-map type management** command.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

The maximum number of policy maps is 64, but you can only apply one policy map per interface. You can apply the same policy map to multiple interfaces. You can identify multiple Layer 3/4 class maps in a Layer 3/4 policy map (see the **class** command), and you can assign multiple actions from one or more feature types to each class map.

Feature Directionality

Actions are applied to traffic bidirectionally or unidirectionally depending on the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions.

Note When you use a global policy, all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally. Because the policy is applied to all interfaces, the policy will be applied in both directions so bidirectionality in this case is redundant.

For features that are applied unidirectionally, for example QoS priority queue, only traffic that enters (or exits, depending on the feature) the interface to which you apply the policy map is affected. See Table 1-1 for the directionality of each feature.

Table 1-1 Feature Directionality

Feature	Single Interface Direction	Global Direction
Application inspection (multiple types)	Bidirectional	Ingress
CSC	Bidirectional	Ingress
IPS	Bidirectional	Ingress
NetFlow Secure Event Logging filtering	N/A	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS standard priority queue	Egress	Egress
QoS traffic shaping, hierarchical priority queue	Egress	Egress
TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
TCP normalization	Bidirectional	Ingress
TCP state bypass	Bidirectional	Ingress

Feature Matching Within a Service Policy

See the following information for how a packet matches class maps in a policy map for a given interface:

1. A packet can match only one class map in the policy map for each feature type.
2. When the packet matches a class map for a feature type, the security appliance does not attempt to match it to any subsequent class maps for that feature type.
3. If the packet matches a subsequent class map for a different feature type, however, then the security appliance also applies the actions for the subsequent class map , if supported. See the "Incompatibility of Certain Feature Actions" section on page 22-59 for more information about unsupported combinations.

For example, if a packet matches a class map for connection limits, and also matches a class map for application inspection, then both actions are applied.

If a packet matches a class map for HTTP inspection, but also matches another class map that includes HTTP inspection, then the second class map actions are not applied.

Note Application inspection includes multiple inspection types, and each inspection type is a separate feature when you consider the matching guidelines above.

Order in Which Multiple Feature Actions are Applied

The order in which different types of actions in a policy map are performed is independent of the order in which the actions appear in the policy map.

Note NetFlow Secure Event Logging filtering is order-independent.

Actions are performed in the following order:

1. QoS input policing
2. TCP normalization, TCP and UDP connection limits and timeouts, TCP sequence number randomization, and TCP state bypass.

Note When a the security appliance performs a proxy service (such as AAA or CSC) or it modifies the TCP payload (such as FTP inspection), the TCP normalizer acts in dual mode, where it is applied before and after the proxy or payload modifying service.

3. CSC
4. Application inspection (multiple types)

   The order of application inspections applied when a class of traffic is classified for multiple inspections is as follows. Only one inspection type can be applied to the same traffic. WAAS inspection is an exception, because it can be applied along with other inspections for the same traffic. See the "Incompatibility of Certain Feature Actions" section on page 22-59 for more information.

   a. CTIQBE
   b. DNS
   c. FTP
   d. GTP
   e. H323
   f. HTTP
   g. ICMP
   h. ICMP error
   i. ILS
   j. MGCP
   k. NetBIOS
   l. PPTP
   m. Sun RPC
   n. RSH
   o. RTSP
   p. SIP
   q. Skinny
   r. SMTP
   s. SNMP

t. SQL*Net
u. TFTP
v. XDMCP
w. DCERPC
x. Instant Messaging

Note RADIUS accounting is not listed because it is the only inspection allowed on management traffic. WAAS is not listed because it can be configured along with other inspections for the same traffic.

5. IPS
6. QoS output policing
7. QoS standard priority queue
8. QoS traffic shaping, hierarchical priority queue

Incompatibility of Certain Feature Actions

Some features are not compatible with each other for the same traffic. For example, you cannot configure QoS priority queueing and QoS policing for the same set of traffic. Also, most inspections should not be combined with another inspection, so the security appliance only applies one inspection if you configure multiple inspections for the same traffic. In this case, the feature that is applied is the higher priority feature in the list in the "Order in Which Multiple Feature Actions are Applied" section on page 22-58.

For information about compatibility of each feature, see the chapter or section for your feature.

Note The **match default-inspection-traffic** command, which is used in the default global policy, is a special CLI shortcut to match the default ports for all inspections. When used in a policy map, this class map ensures that the correct inspection is applied to each packet, based on the destination port of the traffic. For example, when UDP traffic for port 69 reaches the security appliance, then the security appliance applies the TFTP inspection; when TCP traffic for port 21 arrives, then the security appliance applies the FTP inspection. So in this case only, you can configure multiple inspections for the same class map. Normally, the security appliance does not use the port number to determine which inspection to apply, thus giving you the flexibility to apply inspections to non-standard ports, for example.

An example of a misconfiguration is if you configure multiple inspections in the same policy map and do not use the default-inspection-traffic shortcut. In Example 1-1, traffic destined to port 21 is mistakenly configured for both FTP and HTTP inspection. In Example 1-2, traffic destined to port 80 is mistakenly configured for both FTP and HTTP inspection. In both cases of misconfiguration examples, only the FTP inspection is applied, because FTP comes before HTTP in the order of inspections applied.

Example 1-1 Misconfiguration for FTP packets: HTTP Inspection Also Configured

```
class-map ftp
   match port tcp eq 21
class-map http
   match port tcp eq 21 [it should be 80]
policy-map test
   class ftp
     inspect ftp
   class http
     inspect http
```

Example 1-2 Misconfiguration for HTTP packets: FTP Inspection Also Configured

```
class-map ftp
   match port tcp eq 80 [it should be 21]
class-map http
   match port tcp eq 80
policy-map test
   class http
     inspect http
   class ftp
     inspect ftp
```

Feature Matching for Multiple Service Policies

For TCP and UDP traffic (and ICMP when you enable stateful ICMP inspection), service policies operate on traffic flows, and not just individual packets. If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.

For example, if HTTP traffic matches a policy on the inside interface to inspect HTTP traffic, and you have a separate policy on the outside interface for HTTP inspection, then that traffic is not also inspected on the egress of the outside interface. Similarly, the return traffic for that connection will not be inspected by the ingress policy of the outside interface, nor by the egress policy of the inside interface.

For traffic that is not treated as a flow, for example ICMP when you do not enable stateful ICMP inspection, returning traffic can match a different policy map on the returning interface. For example, if you configure IPS on the inside and outside interfaces, but the inside policy uses virtual sensor 1 while the outside policy uses virtual sensor 2, then a non-stateful Ping will match virtual sensor 1 outbound, but will match virtual sensor 2 inbound.

Examples

The following is an example of a **policy-map** command for connection policy. It limits the number of connections allowed to the web server 10.1.1.1:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
hostname(config)# class-map telnet_traffic
```

```
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the security appliance does not make this match because they previously matched other classes.

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
clear configure policy-map	Removes all policy map configuration. If a policy map is in use in a **service-policy** command, that policy map is not removed.
class-map	Defines a traffic class map.
service-policy	Assigns the policy map to an interface or globally to all interfaces.
show running-config policy-map	Display all current policy map configurations.

policy-map type inspect

When using the Modular Policy Framework, define special actions for inspection application traffic by using the **policy-map type inspect** command in global configuration mode. To remove an inspection policy map, use the **no** form of this command.

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

Syntax Description

application	Specifies the type of application traffic you want to act upon. Available types include: • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **radius-accounting** • **sip** • **skinny** • **snmp**
policy_map_name	Specifies the name for this policy map up to 40 characters in length. Names that begin with "_internal" or "_default" are reserved and cannot be used. All types of policy maps use the same name space, so you cannot reuse a name already used by another type of policy map.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine using the **inspect** command in the Layer 3/4 policy map (the **policy-map** command), you can also optionally enable actions as defined in an inspection policy map created by the **policy-map type inspect** command. For example, enter the **inspect http http_policy_map** command where http_policy_map is the name of the inspection policy map.

An inspection policy map consists of one or more of the following commands entered in policy-map configuration mode. The exact commands available for an inspection policy map depends on the application.

- **match** command—You can define a **match** command directly in the inspection policy map to match application traffic to criteria specific to the application, such as a URL string. Then you enable actions in match configuration mode such as **drop**, **reset**, **log**, and so on. The **match** commands available depend on the application.
- **class** command—This command identifies an inspection class map in the policy map (see the **class-map type inspect** command to create the inspection class map). An inspection class map includes **match** commands that match application traffic with criteria specific to the application, such as a URL string, for which you then enable actions in the policy map. The difference between creating a class map and using a **match** command directly in the inspection policy map is that you can group multiple matches, and you can reuse class maps.
- **parameters** command—Parameters affect the behavior of the inspection engine. The commands available in parameters configuration mode depend on the application.

You can specify multiple **class** or **match** commands in the policy map.

Some **match** commands can specify regular expressions to match text inside a packet. See the **regex** command and the **class-map type regex** command, which groups multiple regular expressions.

The default inspection policy map configuration includes the following commands, which sets the maximum message length for DNS packets to be 512 bytes:

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

If a packet matches multiple different **match** or **class** commands, then the order in which the security appliance applies the actions is determined by internal security appliance rules, and not by the order they are added to the policy map. The internal rules are determined by the application type and the logical progression of parsing a packet, and are not user-configurable. For example for HTTP traffic, parsing a Request Method field precedes parsing the Header Host Length field; an action for the Request Method field occurs before the action for the Header Host Length field. For example, the following match commands can be entered in any order, but the **match request method get** command is matched first.

```
hostname(config-pmap)# match request header host length gt 100
hostname(config-pmap-c)# reset
hostname(config-pmap-c)# match request method get
hostname(config-pmap-c)# log
```

If an action drops a packet, then no further actions are performed. For example, if the first action is to reset the connection, then it will never match any further **match** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. (You can configure both the **reset** (or **drop-connection**, and so on.) and the **log** action for the same **match** command, in which case the packet is logged before it is reset for a given match.)

If a packet matches multiple **match** or **class** commands that are the same, then they are matched in the order they appear in the policy map. For example, for a packet with the header length of 1001, it will match the first command below, and be logged, and then will match the second command and be reset. If you reverse the order of the two **match** commands, then the packet will be dropped and the connection reset before it can match the second **match** command; it will never be logged.

```
hostname(config-pmap)# match request header length gt 100
hostname(config-pmap-c)# log
hostname(config-pmap-c)# match request header length gt 1000
hostname(config-pmap-c)# reset
```

A class map is determined to be the same type as another class map or **match** command based on the lowest priority **match** command in the class map (the priority is based on the internal rules). If a class map has the same type of lowest priority **match** command as another class map, then the class maps are matched according to the order they are added to the policy map. If the lowest priority command for each class map is different, then the class map with the higher priority **match** command is matched first.

See the following guidelines when modifying an inspection policy-map:

- HTTP inspection policy maps—If you modify an in-use HTTP inspection policy map (**policy-map type inspect http**), you must remove and reapply the **inspect http** *map* action for the changes to take effect. For example, if you modify the "http-map" inspection policy map, you must remove and readd the **inspect http http-map** command from the layer 3/4 policy:

  ```
  hostname(config)# policy-map test
  hostname(config-pmap)# class http0
  hostname(config-pmap-c)# no inspect http http-map
  hostname(config-pmap-c)# inspect http http-map
  ```

- All inspection policy maps—If you want to exchange an in-use inspection policy map for a different map name, you must remove the **inspect** *protocol map* command, and readd it with the new map. For example:

  ```
  hostname(config)# policy-map test
  hostname(config-pmap)# class sip
  hostname(config-pmap-c)# no inspect sip sip-map1
  hostname(config-pmap-c)# inspect sip sip-map2
  ```

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
```

```
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy inbound_policy interface outside
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
parameters	Enters parameter configuration mode for an inspection policy map.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

policy-server-secret

To configure a secret key used to encrypt authentication requests to the SSO server, use the **policy-server-secret** command in webvpn-sso-siteminder configuration mode. This is an SSO with CA SiteMinder command.

To remove a secret key, use the **no** form of this command.

policy-server-secret *secret-key*

no policy-server-secret

Note This command is required for SSO authentication.

Syntax Description

secret-key	The character string used as a secret key to encrypt authentication communications. There is no minimum or maximum number of characters.

Defaults

No default behavior or value.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn-sso-siteminder configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. You first create the SSO server using the **sso-server** command. The **policy-server-secret** command then secures authentication communications between the security appliance and the SSO server.

The command argument, *secret-key*, is similar to a password: you create it, save it, and configure it. It is configured on both the security appliance using the `policy-server-secret` command and on the SiteMinder Policy Server using the Cisco Java plug-in authentication scheme.

The security appliance currently supports the Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder).

Examples

The following command, entered in webvpn-sso-siteminder configuration mode and including a random character string as an argument, creates a secret key for SSO server authentication communications:

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
hostname(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SSO authentication requests.

polltime interface

To specify the data interface poll and hold times in an Active/Active failover configuration, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface [**msec**] *time* [**holdtime** *time*]

no polltime interface [**msec**] *time* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a data interface must receive a hello message from the peer interface, after which the peer interface is declared failed. Valid values are from 5 to 75 seconds.
interface *time*	Specifies data interface polling period. Valid values are from 3 to 15 seconds. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Defaults

The poll *time* is 5 seconds.

The **holdtime** *time* is 5 times the poll *time*.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The command was changed to include the optional **holdtime** *time* value and the ability to specify the poll time in milliseconds.

Usage Guidelines

Use the **polltime interface** command to change the frequency that hello packets are sent out on interfaces associated with the specified failover group. This command is available for Active/Active failover only. Use the **failover polltime interface** command in Active/Standby failover configurations.

You cannot enter a **holdtime** value that is less than 5 times the poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested. Interface testing begins when a hello packet is not heard on the interface for over half the hold time.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following partial example shows a possible configuration for a failover group. The interface poll time is set to 500 milliseconds and the hold time to 5 seconds for data interfaces in failover group 1.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Specifies the unit failover poll and hold times.
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.

pop3s

To enter POP3S configuration mode, use the **pop3s** command in global configuration mode. To remove any commands entered in POP3S command mode, use the **no** version of this command.

POP3 is a client/server protocol in which your Internet server receives and holds e-mail for you. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. This standard protocol is built into most popular e-mail products. POP3S lets you receive e-mail over an SSL connection.

pop3s

no pop3

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enter POP3S configuration mode:

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.
show running-config pop3s	Displays the running configuration for POP3S.

port

To specify the port an e-mail proxy listens to, use the **port** command in the applicable e-mail proxy command mode. To revert to the default value, use the **no** version of this command.

port {*portnum*}

no port

Syntax Description

portnum	The port for the e-mail proxy to use. To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Defaults

The default ports for e-mail proxies are as follows:

E-mail Proxy	Default Port
IMAP4S	993
POP3S	995
SMTPS	988

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0(1)(1)	This command was introduced.

Usage Guidelines

To avoid conflicts with local TCP services, use port numbers in the range 1024 to 65535.

Examples

The following example shows how to set port 1066 for the IMAP4S e-mail proxy:

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

port-forward

To configure the set of applications that WebVPN users can access over forwarded TCP ports, use the **port-forward** command in global configuration mode. To configure access to multiple applications, use this command with the same listname multiple times, once for each application. To remove an entire configured list, use the **no port-forward** *listname* command. To remove a configured application, use the **no port-forward** *listname localport* command (you need not include the *remoteserver* and *remoteport* parameters).

port-forward {*listname localport remoteserver remoteport description*}

no port-forward *listname*

no port-forward *listname localport*

Syntax Description

description	Provides the application name or short description that displays on the end user Port Forwarding Java applet screen. Maximum 64 characters.
listname	Groups the set of applications (forwarded TCP ports) WebVPN users can access. Maximum 64 characters.
localport	Specifies the local port that listens for TCP traffic for an application. You can use a local port number only once for a *listname*.
remoteport	Specifies the port to connect to for this application on the remote server.
remoteserver	Provides the DNS name or IP address of the remote server for an application. We recommend using DNS names. For more information, see the *Cisco Security Appliance Command Line Configuration Guide*.

Defaults

There is no default port forwarding list.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To allow access to particular TCP port forwarding applications for a specific user or group policy, use the *listname* you create here with the **port-forward** command in webvpn mode.

Examples

The following example shows how to create a portforwarding list called *SalesGroupPorts* that provides access to IMAP4S e-mail, SMTPS e-mail, DDTS, and Telnet. The following table provides values that the example uses for each application.

Application	Local Port	Server DNS Name	Remote Port	Description
IMAP4S e-mail	143	IMAP4Sserver	20143	Get Mail
SMTPS e-mail	25	SMTPSserver	20025	Send Mail
DDTS over SSH	22	DDTSserver	20022	DDTS over SSH
Telnet	23	Telnetserver	20023	Telnet

```
hostname(config)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

Related Commands

Command	Description
clear configuration port-forward [*listname*]	Removes all port forwarding commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
port-forward	Use this command in webvpn mode to enable WebVPN application access for a user or group policy.
show running-config port-forward	Displays the current set of configured **port-forward** commands.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

port-forward (webvpn)

To enable WebVPN application access for this user or group policy, use the **port-forward** command in webvpn mode, which you enter from group-policy or username mode. To remove the port forwarding attribute from the configuration, including a null value created by issuing the **port-forward none** command, use the **no** form of this command. The **no** option allows inheritance of a list from another group policy. To prevent inheriting a port forwarding list, use the **port-forward none** command.

port-forward {**value** *listname* | **none**}

no port-forward

Syntax Description

none	Indicates that there is no filtering. Sets a null value, thereby disallowing a filtering. Prevents inheriting filtering values.
value listname	Identifies the list of applications WebVPN users can access. Use the port-forward command in configuration mode to define the list.

Defaults

Port forwarding is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **port-forward command** in webvpn mode to enable application access, you must define a list of applications that you want users to be able to use in a WebVPN connection. Use the **port-forward** command in global configuration mode to define this list.

Examples

The following example shows how to set a portforwarding list called *ports1* for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
```

Related Commands

Command	Description
clear configuration port-forward [*listname*]	Removes all port forwarding commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
port-forward	Use this command in configuration mode to define applications, or forwarded ports, that WebVPN users can access.
show running-config port-forward	Displays the current set of configured **port-forward** commands.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

port-forward-name

To configure the display name that identifies TCP port forwarding to end users for a particular user or group policy, use the **port-forward-name** command in webvpn mode, which you enter from group-policy or username mode. To delete the display name, including a null value created by using the **port-forward-name none** command**,** use the no form of the command. The **no** option restores the default name, "Application Access." To prevent a display name, use the **port-forward none** command.

port-forward-name {**value** *name* | **none**}

no port-forward-name

Syntax Description

none	Indicates that there is no display name. Sets a null value, thereby disallowing a display name. Prevents inheriting a value.
value *name*	Describes port forwarding to end users. Maximum of 255 characters.

Defaults

The default name is "Application Access."

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set the name, "Remote Access TCP Applications," for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

Related Commands

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

port-object

To add a port object to a service object group, use the **port-object** command in service configuration mode. To remove port objects, use the **no** form of this command.

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

Syntax Description

begin_service	Specifies the decimal number or name of a TCP or UDP port that is the beginning value for a range of services. This value must be between 0 and 65535.
end_service	Specifies the decimal number or name of a TCP or UDP port that is the ending value for a range of services. ervices. This value must be between 0 and 65535.
eq service	Specifies the decimal number or name of a TCP or UDP port for a service object.
range	Specifies a range of ports (inclusive).

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **port-object** command is used with the **object-group** command to define an object that is either a specific service (port) or a range of services (ports) in service configuration mode.

If a name is specified for a TCP or UDP service, it must be one of the supported TCP or/and UDP names, and must be consistent with the protocol type of the object group. For instance, for a protocol types of tcp, udp, and tcp-udp, the names must be a valid TCP service name, a valid UDP service name, or a valid TCP and UDP service name, respectively.

If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object.

The following service names are supported:

Table 1-3

TCP	UDP	TCP and UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

This example shows how to use the **port-object** command in service configuration mode to create a new port (service) object group:

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
```

```
hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

Related Commands

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

pppoe client route distance

To configure an administrative distance for routes learned through PPPoE, use the **pppoe client route distance** command in interface configuration mode. To restore teh default setting, use the **no** form of this command.

pppoe client route distance *distance*

no pppoe client route distance *distance*

Syntax Description

distance	The administrative distance to apply to routes learned through PPPoE. Valid values are from 1 to 255.

Defaults

Routes learned through PPPoE are given an administrative distance of 1 by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client route distance** command is checked only when a route is learned from PPPoE. If the **pppoe client route distance** command is entered after a route is learned from PPPoE, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enablgin PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client route track

To configure the PPPoE client to associate added routes with a specified tracked object number, use the **pppoe client route track** command in interface configuration mode. To remove the PPPoE route tracking, use the **no** form of this command.

pppoe client route track *number*

no pppoe client route track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client route track** command is checked only when a route is learned from PPPoE. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
```

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

pppoe client secondary

To configure the PPPoE client to register as a client of a tracked object and to be brought up or down based on the tracking state, use the **pppoe client secondary** command in interface configuration mode. To remove the client registration, use the **no** form of this command.

pppoe client secondary track *number*

no pppoe client secondary track

Syntax Description

number	The tracking entry object ID. Valid values are from 1 to 500.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **pppoe client secondary** command is checked only when PPPoE session starts. If the **pppoe client route track** command is entered after a route is learned from PPPoE, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address pppoe** command to obtain routes through PPPoE.

If PPPoE is configured on multiple interfaces, you must use the **pppoe client route distance** command on each of the interfaces to indicate the priority of the installed routes. Enabling PPPoE clients on multiple interfaces is only supported with object tracking.

You cannot configure failover if you obtain IP addresses using PPPoE.

Examples

The following example obtains the default route through PPPoE on GigabitEhternet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the secondary route obtained on GigabitEthernet0/3 through PPPoE is used.

```
hostname(config)# sla monitor 123
```

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

Related Commands

Command	Description
ip address pppoe	Configures the specified interface with an IP address obtained through PPPoE.
ppoe client secondary	Configures tracking for secondary PPPoE client interface.
pppoe client route distance	Assigns an administrative distance to routes learned through PPPoE.
pppoe client route track	Associates routes learned through PPPoE with a tracking entry object.
sla monitor	Defines an SLA monitoring operation.

preempt

To cause the unit to become active on boot if it has the higher priority, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]

no preempt [*delay*]

Syntax Description

seconds	The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Defaults

By default, there is no delay.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). However, if one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Note If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
hostname(config)# failover group 1
```

```
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

To create an entry in a prefix list for ABR type 3 LSA filtering, use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

Syntax Description

/	A required separator between the *network* and *len* values.
deny	Denies access for a matching condition.
ge *min_value*	(Optional) Specifies the minimum prefix length to be matched. The value of the *min_value* argument must be greater than the value of the *len* argument and less than or equal to the *max_value* argument, if present.
le *max_value*	(Optional) Specifies the maximum prefix length to be matched. The value of the *max_value* argument must be greater than or equal to the value of the *min_value* argument, if present, or greater than the value of the *len* argument if the *min_value* argument is not present.
len	The length of the network mask. Valid values are from 0 to 32.
network	The network address.
permit	Permits access for a matching condition.
prefix-list-name	The name of the prefix list. The prefix-list name cannot contain spaces.
seq *seq_num*	(Optional) Applies the specified sequence number to the prefix list being created.

Defaults

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The security appliance begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a mach is made, the security appliance does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified.The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

len < *min_value* <= *max_value* <= 32

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix10.0.0.0/8:

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

prefix-list-name	The name of a prefix list.
text	The text of the prefix list description. You can enter a maximum of 80 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
```

!

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Defaults

Prefix list sequence numbering is enabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Only the **no** form of this command appears in the configuration. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples

The following example disables prefix list sequence numbering:

```
hostname(config)# no prefix-list sequence-number
```

Related Commands

Command	Description
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

pre-shared-key

To specify a preshared key to support IKE connections based on preshared keys, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

pre-shared-key *key*

no pre-shared-key

Syntax Description

key	Specifies an alphanumeric key between 1 and 128 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following command entered in config-ipsec configuration mode, specifies the preshared key XYZX to support IKE connections for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

primary

To give the primary unit higher priority for a failover group, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary

no primary

Syntax Description

This command has no arguments or keywords.

Defaults

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). If one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
```

```
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
secondary	Gives the secondary unit a higher priority than the primary unit.

priority (class)

To enable QoS priority queueing, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queueing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or variables.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface (see the **priority-queue** command), while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue (the **shape** command). A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queueing:
  - Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.

- Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
- For IPSec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
- IPSec-over-TCP is not supported for priority traffic classification.

Configuring QoS with Modular Policy Framework

To enable priority queueing, use the Modular Policy Framework. You can use standard priority queueing or hierarchical priority queueing.

For standard priority queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

For hierarchical priority-queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.
   c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following is an example of the **priority** command in policy-map mode:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

Related Commands

class	Specifies a class map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.

policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

priority (vpn load balancing)

To set the priority of the local device participating in the virtual load-balancing cluster, use the **priority** command in VPN load-balancing mode. To revert to the default priority specification, use the **no** form of this command.

priority *priority*

no priority

Syntax Description

priority	The priority, in the range of 1 to 10, that you want to assign to this device.

Defaults

The default priority depends on the model number of the device:

Model Number	Default Priority
5520	5
5540	7

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter VPN load-balancing mode.

This command sets the priority of the local device participating in the virtual load-balancing cluster.

The priority must be an integer in the range of 1 (lowest) to 10 (highest).

The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster. See *Cisco Security Appliance Command Line Configuration Guide* for details about the master-election process.

The **no** form of the command reverts the priority specification to the default value.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **priority** command that sets the priority of the current device to 9:

```
hostname(config)# interface GigabitEthernet 0/1
```

```
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

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

priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

priority-queue *interface-name*

no priority queue *interface-name*

Syntax Description

interface-name	Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505, the name of the VLAN interface.

Defaults

By default, priority queuing is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The security appliance supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface that yopu create using the **priority-queue** command, while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size (the **queue-limit** command). You can also fine-tune the maximum number of packets allowed into the transmit queue (the **tx-ring-limit** command). These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.
- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used.

On ASA Model 5505 (only), configuring priority-queue on one interface overwrites the same configuration on all other interfaces. That is, only the last applied configuration is present on all interfaces. Further, if the priority-queue configuration is removed from one interface, it is removed from all interfaces.

To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue-limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

Related Commands

Command	Description
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure priority-queue	Removes the current priority queue configuration.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.

privilege

To configure the command privilege levels, use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

no privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege level for the **clear** command corresponding to the command specified.
command *command*	Specifies the command on which to set the privilege level.
configure	(Optional) Sets the privilege level for the command specified.
level *level*	Specifies the privilege level; valid values are from 0 to 15.
mode enable	(Optional) Indicates that the level is for the enable mode of the command.
mode configure	(Optional) Indicates that the level is for the configure mode of the command.
show	(Optional) Sets the privilege level for the **show** command corresponding to the command specified.

Defaults

No default behaviors or values.

Command Modes

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

	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 privilege command lets you set user-defined privilege levels for the security appliance **commands. In particular, this command is useful for setting different privilege levels for related configuration, show, and clear commands. Make sure that you** verify privilege level changes in your commands with your security policies before using the new privilege levels.

When commands and users have privilege levels set, the two are compared to determine if a given user can execute a given command. If the user's privilege level is lower than the privilege level of the command, the user is prevented from executing the command.

To change between privilege levels, use the **login** command to access another privilege level and the appropriate **logout**, **exit**, or **quit** command to exit that level.

The **mode enable** and **mode configure** keywords are for commands with both enable and configure modes.

Lower privilege level numbers are lower privilege levels.

Note The **aaa authentication** and **aaa authorization** commands need to include any new privilege levels that you define before you can use them in your AAA server configuration.

Examples

This example shows how to set the privilege level "5" for an individual user as follows:

```
username intern1 password pass1 privilege 5
```

This example shows how to define a set of **show** commands with the privilege level "5" as follows:

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
hostname(config)#
```

This example shows how to apply privilege level 11 to a complete AAA authorization configuration:

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
hostname(config)#
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show curpriv	Display current privilege level.
show running-config privilege	Display privilege levels for commands.

prompt

To configure the session prompt display, use the **prompt** command in configuration mode (P_CONF), replicated (P_REP) and in single mode, and in the system context in multi-mode. Only an administrator can view the configured prompt. If you are in user context, you can see the default hostname/context (config-mode) prompt.

prompt [<*keyword*> [*keyword*>] ...]

no prompt

Syntax Description

Keyword	Description
context	Configures the prompt to display the current context (multimode only).
domain	Configures the prompt to display the domain.
hostname	Configures the prompt to display the hostname.
priority	Configures the prompt to display the 'failover lan unit' setting.
state	Configures the prompt to display the current traffic handling state. The following values maybe e displayed for the *state* keyword: *act* - unit is in traffic passing state, such as Active with failover enabled *stby* - unit is not in traffic passing state, could be standby, failed, or other non-active state *actNoFailover*- non-failover configuration with unit able to pass traffic

Defaults

The default is hostname/context prompt.

Command Modes

The following table shows the modes in which 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 ability to add information to a prompt allows you to see at-a-glance which module you are logged into when you have multiple modules. During a failover, this is important where both modules have the same hostname.

Examples

The following example shows how to configure a prompt:

```
asa (config)# prompt hostname context priority state
```

Assume:

```
hostname = myasa
context = admin
priority = failover lan unit primary
state = Active (with failover enabled)
```

Prompt will display:

```
myasa/admin/pri/act>
myasa/admin/pri/act#
myasa/admin/pri/act(config)#
myasa/admin/pri/act(config-interface)#
```

Help and usage:

```
asa# help prompt

asa# prompt ?

configure mode commands/options:
hostname    Configures the prompt to display the hostname
domain       Configures the prompt to display the domain
context       Configures the prompt to display the current context (multimode only)
priority       Configures the prompt to display the 'failover lan unit' setting
state           Configures the prompt to display the current traffic handling state
```

Related Commands

Command	Description
clear config prompt	Clears the configured prompt.
no prompt	Removes the prompt completely.
show running-config prompt	Displays the configured prompt.

protocol-enforcement

To enable the domain name, label length, and format check, including compression and looped pointer check, use the **protocol-enforcement** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

protocol-enforcement

no protocol-enforcement

Syntax Description

This command has no arguments or keywords.

Defaults

Protocol enforcement is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no protocol-enforcement** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Under certain conditions, protocol enforcement is performed even if the command is disabled. This occurs when parsing a DNS resource record is required for other purposes, such as DNS resource record classification, NAT or TSIG check.

Examples

The following example shows how to enable protocol enforcement in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

protocol http

no protocol http

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit HTTP.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you use this command, be sure to assign HTTP rules to the public interface filter.

Examples

The following example enters ca-crl configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol ldap

no protocol ldap

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit LDAP.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in crl configure mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol scep

no protocol scep

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit SCEP.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol ldap	Specifies LDAP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the **protocol-object** command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*

no protocol-object *protocol*

Syntax Description

protocol	Protocol name or number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

Related Commands

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

protocol-violation

To define actions when a protocol violation occurs with HTTP and NetBIOS inspection, use the **protocol-violation** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

protocol-violation action [drop | log]

no protocol-violation action [drop | log]

Syntax Description

drop	Specifies to drop packets that do not conform to the protocol.
log	Specifies to log the protocol violations.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an HTTP or NetBIOS policy map. A syslog is issued when the HTTP or NetBIOS parser cannot detect a valid HTTP or NetBIOS message in the first few bytes of the message. This occurs, for instance, when a chunked encoding is malformed and the message cannot be parsed.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation action drop
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

proxy-bypass

To configure the security appliance to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML—use the **proxy-bypass** command in webvpn mode. To disable proxy bypass, use the **no** form of the command.

proxy-bypass interface *interface name* **{port** *port number***| path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* **{port** *port number***| path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

Syntax Description

host	Identifies the host to forward traffic to. Use either the host IP address or a hostname.
interface	Identifies the ASA interface for proxy bypass.
interface name	Specifies an ASA interface by name.
link	Specifies rewriting of absolute external links.
none	Specifies no rewriting.
path-mask	Specifies the pattern to match.
path-mask	Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 128 bytes.
port	Identifies the port reserved for proxy bypass.
port number	Specifies a high numbered port reserved for proxy bypass. The port range is 20000-21000. You can use a port for one proxy bypass rule only.
rewrite	(Optional) Specifies the additional rules for rewriting: none or a combination of XML and links.
target	Identifies the remote server to forward the traffic to.
url	Enter the URL in the format **http(s)://***fully_qualified_domain_name*[:*port*]. Maximum 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
xml	Specifies rewriting XML content.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use proxy bypass for applications and web resources that work better with minimum content rewriting. The proxy-bypass command determines how to treat specific web applications that travel through the security appliance.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the security appliance. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.mycompany.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.mycompany.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

Examples

The following example shows how to configure the security appliance to use port 20001 for proxy bypass over the webvpn interface, using HTTP and its default port 80, to forward traffic to mycompany.site.com and to rewrite XML content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://mycompany.site.com rewrite xml
hostname(config-webvpn)#
```

The next example shows how to configure the security appliance to use the path mask mypath/* for proxy bypass on the outside interface, using HTTP and its default port 443 to forward traffic to mycompany.site.com, and to rewrite XML and link content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://mycompany.site.com rewrite xml,link
hostname(config-webvpn)#
```

Related Commands-

Command	Description
apcf	Specifies nonstandard rules to use for a particular application
rewrite	Determines whether traffic travels through the security appliance.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

The root directory (/) is the default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is similar in functionality to the **dir** command.

Examples

The following example shows how to display the current working directory:

```
hostname# pwd
flash:
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
more	Displays the contents of a file.