CHAPTER 32

tcp-map through type echo Commands

tcp-map

To define a set of TCP normalization actions, use the **tcp-map** command in global configuration mode. The TCP normalization feature lets you specify criteria that identify abnormal packets, which the security appliance drops when they are detected. To remove the TCP map, use the **no** form of this command.

tcp-map *map_name*

no tcp-map *map_name*

Syntax Description

map_name	Specifies the TCP map name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This feature uses Modular Policy Framework. First define the TCP normalization actions you want to take using the **tcp-map** command. The **tcp-map** command enters tcp-map configuration mode, where you can enter one or more commands to define the TCP normalization actions. Then define the traffic to which you want to apply the TCP map using the **class-map** command. Enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, enter the **set connection advanced-options** command to reference the TCP map. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco Security Appliance Command Line Configuration Guide*.

The following commands are available in tcp-map configuration mode:

check-retransmission	Enables and disables the retransmit data checks.
checksum-verification	Enables and disable checksum verification.
exceed-mss	Allows or drops packets that exceed MSS set by peer.

queue-limit	Configures the maximum number of out-of-order packets that can be queued for a TCP connection. This command is only available on the ASA 5500 series adaptive security appliance. On the PIX 500 series security appliance, the queue limit is 3 and cannot be changed.
reserved-bits	Sets the reserved flags policy in the security appliance.
syn-data	Allows or drops SYN packets with data.
tcp-options	Allows or clears the selective-ack, timestamps, or window-scale TCP options.
ttl-evasion-protection	Enables or disables the TTL evasion protection offered by the security appliance.
urgent-flag	Allows or clears the URG pointer through the security appliance.
window-variation	Drops a connection that has changed its window size unexpectedly.

Examples

For example, to allow urgent flag and urgent offset packets for all traffic sent to the range of TCP ports between the well known FTP data port and the Telnet port, enter the following commands:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow

hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet

hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap

hostname(config-pmap-c)# service-policy pmap global
```

Related Commands

Command	Description
class (policy-map)	Specifies a class map to use for traffic classification.
clear configure tcp-map	Clears the TCP map configuration.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config tcp-map	Displays the information about the TCP map configuration.
tcp-options	Allows or clears the selective-ack, timestamps, or window-scale TCP options.

tcp-options

To allow or clear the TCP options through the security appliance, use the **tcp-options** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

no tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

tcp-options range *lower upper* {**allow** | **clear** | **drop**}

no tcp-options range *lower upper* {**allow** | **clear** | **drop**}

Syntax Description

allow	Allows the TCP options through the TCP normalizer.
clear	Clears the TCP options through the TCP normalizer and allows the packet.
drop	Drops the packet.
lower	Lower bound ranges (6-7) and (9-255).
selective-ack	Sets the selective acknowledgement mechanism (SACK) option. The default is to allow the SACK option.
timestamp	Sets the timestamp option. Clearing the timestamp option will disable PAWS and RTT. The default is to allow the timestamp option.
upper	Upper bound range (6-7) and (9-255).
window-scale	Sets the window scale mechanism option. The default is to allow the window scale mechanism option.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **tcp-options** command in tcp-map configuration mode to clear selective-acknowledgement, window-scale, and timestamp TCP options. You can also clear or drop packets with options that are not very well defined.

Examples

The following example shows how to drop all packets with TCP options in the ranges of 6-7 and 9-255:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# tcp-options range 6 7 drop
hostname(config-tcp-map)# tcp-options range 9 255 drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

telnet

To add Telnet access to the console and set the idle timeout, use the **telnet** command in global configuration mode. To remove Telnet access from a previously set IP address, use the **no** form of this command.

telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

no telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

Syntax Description

hostname	Specifies the name of a host that can access the Telnet console of the security appliance.
interface_name	Specifies the name of the network interface to Telnet to.
IP_address	Specifies the IP address of a host or network authorized to log in to the security appliance.
IPv6_address	Specifies the IPv6 address/prefix authorized to log in to the security appliance.
mask	Specifies the netmask associated with the IP address.
timeout *number*	Number of minutes that a Telnet session can be idle before being closed by the security appliance; valid values are from 1 to 1440 minutes.

Defaults

By default, Telnet sessions left idle for five minutes are closed by the security appliance.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The variable *IPv6_address* was added. The **no telnet timeout** command was added too.

Usage Guidelines

The **telnet** command lets you specify which hosts can access the security appliance console with Telnet. You can enable Telnet to the security appliance on all interfaces. However, the security appliance enforces that all Telnet traffic to the outside interface be protected by IPSec. To enable a Telnet session to the outside interface, configure IPSec on the outside interface to include IP traffic that is generated by the security appliance and enable Telnet on the outside interface.

Use the **no telnet** command to remove Telnet access from a previously set IP address. Use the **telnet timeout** command to set the maximum time that a console Telnet session can be idle before being logged off by the security appliance. You cannot use the **no telnet** command with the **telnet timeout** command.

If you enter an IP address, you must also enter a netmask. There is no default netmask. Do not use the subnetwork mask of the internal network. The *netmask* is only a bit mask for the IP address. To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255.

If IPSec is operating, you can specify an unsecure interface name, which is typically, the outside interface. At a minimum, you might configure the **crypto map** command to specify an interface name with the **telnet** command.

Use the **passwd** command to set a password for Telnet access to the console. The default is **cisco**. Use the **who** command to view which IP addresses are currently accessing the security appliance console. Use the **kill** command to terminate an active Telnet console session.

If you use the **aaa** command with the **console** keyword, Telnet console access must be authenticated with an authentication server.

Note If you have configured the **aaa** command to require authentication for security appliance Telnet console access and the console login request times out, you can gain access to the security appliance from the serial console by entering the security appliance username and the password that was set with the **enable password** command.

Examples

This example shows how to permit hosts 192.168.1.3 and 192.168.1.4 to access the security appliance console through Telnet. In addition, all the hosts on the 192.168.2.0 network are given access.

```
hostname(config)# telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# telnet 192.168.1.4 255.255.255.255 inside
hostname(config)# telnet 192.168.2.0 255.255.255.0 inside
hostname(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

This example shows how to change the maximum session idle duration:

```
hostname(config)# telnet timeout 10
hostname(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

This example shows a Telnet console login session (the password does not display when entered):

```
hostname# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
hostname>
```

You can remove individual entries with the **no telnet** command or all telnet command statements with the **clear configure telnet** command:

```
hostname(config)# no telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

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

Related Commands

Command	Description
clear configure telnet	Removes a Telnet connection from the configuration.
kill	Terminates a Telnet session.
show running-config telnet	Displays the current list of IP addresses that are authorized to use Telnet connections to the security appliance.
who	Displays active Telnet administration sessions on the security appliance.

terminal

To allow system log messages to show in the current Telnet session, use the **terminal monitor** command in privileged EXEC mode. To disable the display of system log messages, use the **terminal no monitor** command.

terminal {**monitor** | **no monitor**}

Syntax Description

monitor	Enables the display of system log messages in the current Telnet session.
no monitor	Disables the display of system log messages in the current Telnet session.

Defaults

System log messages are disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to enable and disable the display of system log messages in the current session:

```
hostname# terminal monitor
hostname# terminal no monitor
```

Related Commands

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

terminal pager

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

terminal pager [lines] *lines*

Syntax Description

[**lines**] *lines*	(Optional) Sets the number of lines on a page before the "---more---" prompt appears. The default is 24 lines; zero indicates no page limit. The range is 0 through 2147483647 lines.

Defaults

The default is 24 lines.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command changes the pager line setting only for the current Telnet session. To save a new default pager setting to the configuration, use the **pager** command.

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

Examples

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

```
hostname# terminal pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is saved to the configuration.

Command	Description
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messsages to display in the Telnet session.
terminal width	Sets the terminal display width.

terminal width

To set the width for displaying information during console sessions, use the **terminal width** command in global configuration mode. To disable, use the **no** form of this command.

terminal width *columns*

no terminal width *columns*

Syntax Description

columns	Specifies the terminal width in columns. The default is 80. The range is 40 to 511.

Defaults

The default display width is 80 columns.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to terminal display width to 100 columns:

```
hostname# terminal width 100
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Sets the terminal line parameters in privileged EXEC mode.

test aaa-server

To check whether the security appliance can authenticate or authorize users with a particular AAA server, use the **test aaa-server** command in privileged EXEC mode. Failure to reach the AAA server may be due to incorrect configuration on the security appliance, or the AAA server may be unreachable for other reasons, such as restrictive network configurations or server downtime.

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*]}

Syntax Description

authentication	Tests a AAA server for authentication capability.
authorization	Tests a AAA server for legacy VPN authorization capability.
host *ip_address*	Specifies the server IP address. If you do not specify the IP address in the command, you are prompted for it.
password *password*	Specifies the user password. If you do not specify the password in the command, you are prompted for it.
server_tag	Specifies the AAA server tag as set by the **aaa-server** command.
username *username*	Specifies the username of the account used to test the AAA server settings. Make sure the username exists on the AAA server; otherwise, the test will fail. If you do not specify the username in the command, you are prompted for it.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **test aaa-server** command lets you verify that the security appliance can authenticate users with a particular AAA server, and for legacy VPN authorization, if you can authorize a user. This command lets you test the AAA server without having an actual user who attempts to authenticate or authorize. It also helps you isolate whether AAA failures are due to misconfiguration of AAA server parameters, a connection problem to the AAA server, or other configuration errors on the security appliance.

Examples

The following example configures a RADIUS AAA server named srvgrp1 on host 192.168.3.4, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650. The **test aaa-server** command following the setup of the AAA server parameters indicates that the authentication test failed to reach the server.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

The following is sample output from the **test aaa-server** command with a successful outcome:

```
hostname# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

Related Commands

Command	Description
aaa authentication console	Configures authentication for management traffic.
aaa authentication match	Configures authentication for through traffic.
aaa-server	Creates a AAA server group.
aaa-server host	Adds a AAA server to a server group.

test dynamic-access-policy attributes

To enter the dap attributes mode, from Privileged EXEC mode, enter the **test dynamic-access-policy attributes** command. Doing so lets you specify user and endpoint attribute value pairs.

dynamic-access-policy attributes

Defaults

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Normally the security appliance retrieves user authorization attributes from the AAA server and retrieves endpoint attributes from Cisco Secure Desktop, Host Scan, CNA or NAC. For the test command, you specify the user authorization and endpoint attributes in this attributes mode. The security appliance writes them to an attribute database that the DAP subsystem references when evaluating the AAA selection attributes and endpoint select attributes for a DAP record.

This feature lets you experiment with creating a DAP record.

Examples

The following example shows how to use the **attributes** command.

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
attributes	Enters attributes mode, in which you can specify user attribute value pairs.
display	Displays current attribute list.

test dynamic-access-policy execute

test regex

To test a regular expression, use the **test regex** command in privileged EXEC mode.

test regex *input_text regular_expression*

Syntax Description

input_text	Specifies the text that you want to match with the regular expression.
regular_expression	Specifies the regular expression up to 100 characters in length. See the **regex** command for a list of metacharacters you can use in the regular expression.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **test regex** command tests a regular expression to make sure it matches what you think it will match.

If the regular expression matches the input text, you see the following message:

```
INFO: Regular expression match succeeded.
```

If the regular expression does not match the input text, you see the following message:

```
INFO: Regular expression match failed.
```

Examples

The following example tests input text against a regular expression:

```
hostname# test regex farscape scape
INFO: Regular expression match succeeded.

hostname# test regex farscape scaper

INFO: Regular expression match failed.
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
class-map type regex	Creates a regular expression class map.
regex	Creates a regular expression.

test sso-server

To test an SSO server with a trial authentication request, use the **test sso-server** command in privileged EXEC mode.

test sso-server *server-name* **username** *user-name*

Syntax Description

server-name	Specifies the name of the SSO server being tested.
user-name	Specifies the name of a user on the SSO server being tested.

Defaults

No default values or behavior.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn	•	—	•	—	—
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
Global configuration mode	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **test sso-server** command tests whether an SSO server is recognized and responding to authentication requests.

If the SSO server specified by the *server-name* argument is not found, the following error appears:

```
ERROR: sso-server server-name does not exist
```

If the SSO server is found but the user specified by the *user-name* argument is not found, the authentication is rejected.

In the authentication, the security appliance acts as a proxy for the WebVPN user to the SSO server. The security appliance currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. This command applies to both types of SSO Servers.

Examples

The following example, entered in privileged EXEC mode, successfully tests an SSO server named my-sso-server using a username of Anyuser:

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
hostname#
```

The following example shows a test of the same server, but the user, Anotheruser, is not recognized and the authentication fails:

```
hostname# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
hostname#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SiteMinder SSO authentication requests.

text-color

To set a color for text in the WebVPN title bar on the login, home page, and file access page, use the **text-color** command in webvpn mode. To remove a text color from the configuration and reset the default, use the no form of this command.

text-color [*black* | *white* | *auto*]

no text-color

Syntax Description

auto	Chooses black or white based on the settings for the secondary-color command. That is, if the secondary color is black, this value is white.
black	The default text color for title bars is white.
white	You can change the color to black.

Defaults

The default text color for the title bars is white.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set the text color for title bars to black:

```
hostname(config)# webvpn
hostname(config-webvpn)# text-color black
```

Related Commands

Command	Description
secondary-text-color	Sets the secondary text color for the WebVPN login, home page, and file access page.

tftp-server

To specify the default TFTP server, and the path and filename for use with the **configure net** or **write net** commands, use the **tftp-server** command in global configuration mode. To remove the server configuration, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

Syntax Description

interface_name	Specifies the gateway interface name. If you specify an interface other than the highest security interface, a warning message informs you that the interface is not secure.
server	Sets the TFTP server IP address or name. You can enter an IPv4 or IPv6 address.
filename	Specifies the path and filename.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The gateway interface is now required.

Usage Guidelines

The **tftp-server** command simplifies entering the **configure net** and **write net** commands. When you enter the **configure net** or **write net** commands, you can either inherit the TFTP server specified by the **tftp-server** command, or provide your own value. You can also inherit the path in the **tftp-server** command as is, add a path and filename to the end of the **tftp-server** command value, or override the **tftp-server** command value.

The security appliance supports only one **tftp-server** command.

Examples

This example shows how to specify a TFTP server and then read the configuration from the /temp/config/test_config directory:

```
hostname(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
hostname(config)# configure net
```

Related Commands

Command	Description
configure net	Loads the configuration from the TFTP server and path that you specify.
show running-config tftp-server	Displays the default TFTP server address and the directory of the configuration file.

threat-detection basic-threat

To enable basic threat detection, use the **threat-detection basic-threat** command in global configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection basic-threat

no threat-detection basic-threat

Syntax Description

This command has no arguments or keywords.

Defaults

Basic threat detection is enabled by default. The following default rate limits are used:

Table 32-1 Basic Threat Detection Default Settings

	Trigger Settings	
Packet Drop Reason	**Average Rate**	**Burst Rate**
• DoS attack detected • Bad packet format • Connection limits exceeded • Suspicious ICMP packets detected	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 10 second period.
	80 drops/sec over the last 3600 seconds.	320 drops/sec over the last 60 second period.
Scanning attack detected	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
	4 drops/sec over the last 3600 seconds.	8 drops/sec over the last 60 second period.
Incomplete session detected such as TCP SYN attack detected or no data UDP session attack detected (combined)	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 10 second period.
	80 drops/sec over the last 3600 seconds.	160 drops/sec over the last 60 second period.
Denial by access lists	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 10 second period.
	320 drops/sec over the last 3600 seconds.	640 drops/sec over the last 60 second period.
• Basic firewall checks failed • Packets failed application inspection	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 10 second period.
	320 drops/sec over the last 3600 seconds.	1280 drops/sec over the last 60 second period.
Interface overload	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 10 second period.
	1600 drops/sec over the last 3600 seconds.	6400 drops/sec over the last 60 second period.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

When you enable basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the following reasons:

- Denial by access lists
- Bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length)
- Connection limits exceeded (both system-wide resource limits, and limits set in the configuration)
- DoS attack detected (such as an invalid SPI, Stateful Firewall check failure)
- Basic firewall checks failed (This option is a combined rate that includes all firewall-related packet drops in this bulleted list. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.)
- Suspicious ICMP packets detected
- Packets failed application inspection
- Interface overload
- Scanning attack detected (This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.)
- Incomplete session detection such as TCP SYN attack detected or no data UDP session attack detected

When the security appliance detects a threat, it immediately sends a system log message (733100) and alerts ASDM.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 32-1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command. You can override the default settings for each type of event by using the **threat-detection rate** command.

If an event rate is exceeded, then the security appliance sends a system message. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. The burst event rate is 1/60th of the average rate interval or 10 seconds, whichever is higher. For each event received, the security appliance checks the average and burst rate limits; if both rates are exceeded, then the security appliance sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can change the default rate limits for each event type using the **threat-detection rate** command in global configuration mode. If you enable scanning threat detection using the **threat-detection scanning-threat** command, then this command with the **scanning-threat** keyword also sets the when a host is considered to be an attacker or a target; otherwise the default **scanning-threat** value is used for both basic and scanning threat detection. To return to the default setting, use the **no** form of this command.

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

Syntax Description

acl-drop	Sets the rate limit for dropped packets caused by denial by access lists.
average-rate *av_rate*	Sets the average rate limit between 0 and 2147483647 in drops/sec.
bad-packet-drop	Sets the rate limit for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
burst-rate *burst_rate*	Sets the burst rate limit between 0 and 2147483647 in drops/sec. The burst rate is calculated as the average rate every *N* seconds, where *N* is the burst rate interval. The burst rate interval is 1/60th of the **rate-interval** *rate_interval* value or 10 seconds, whichever is larger.
conn-limit-drop	Sets the rate limit for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	Sets the rate limit for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	Sets the rate limit for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop**, **inspect-drop**, and **scanning-threat**.
icmp-drop	Sets the rate limit for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	Sets the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	Sets the rate limit for dropped packets caused by an interface overload.
rate-interval *rate_interval*	Sets the average rate interval between 600 seconds and 2592000 seconds (30 days). The rate interval is used to determine the length of time over which to average the drops. It also determines the burst threshold rate interval.

scanning-threat	Sets the rate limit for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	Sets the rate limit for dropped packets caused by an incomplete session, such as TCP SYN attack or no data UDP session attack.

Defaults

When you enable basic threat detection using the **threat-detection basic-threat** command, the following default rate limits are used:

Table 32-2 Basic Threat Detection Default Settings

	Trigger Settings	
Packet Drop Reason	**Average Rate**	**Burst Rate**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 10 second period.
	100 drops/sec over the last 3600 seconds.	400 drops/sec over the last 60 second period.
scanning-threat	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
	5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 60 second period.
syn-attack	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 10 second period.
	100 drops/sec over the last 3600 seconds.	200 drops/sec over the last 60 second period.
acl-drop	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 10 second period.
	400 drops/sec over the last 3600 seconds.	800 drops/sec over the last 60 second period.
• **fw-drop** • **inspect-drop**	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 10 second period.
	400 drops/sec over the last 3600 seconds.	1600 drops/sec over the last 60 second period.
interface-drop	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 10 second period.
	2000 drops/sec over the last 3600 seconds.	8000 drops/sec over the last 60 second period.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can configure up to three different rate intervals for each event type.

When you enable basic threat detection, the security appliance monitors the rate of dropped packets and security events due to the event types described in the "Syntax Description" table.

When the security appliance detects a threat, it immediately sends a system log message (733100) and alerts ASDM.

Basic threat detection affects performance only when there are drops or potential threats; even in this scenario, the performance impact is insignificant.

Table 32-1 in the "Defaults" section lists the default settings. You can view all these default settings using the **show running-config all threat-detection** command.

If an event rate is exceeded, then the security appliance sends a system message. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event received, the security appliance checks the average and burst rate limits; if both rates are exceeded, then the security appliance sends two separate system messages, with a maximum of one message for each rate type per burst period.

Examples

The following example enables basic threat detection, and changes the triggers for DoS attacks:

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection rate	Shows basic threat detection statistics.
threat-detection basic-threat	Enables basic threat detection.
threat-detection scanning-threat	Enables scanning threat detection.

threat-detection scanning-threat

To enable scanning threat detection, use the **threat-detection scanning-threat** command in global configuration mode. To disable scanning threat detection, use the **no** form of this command.

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

Syntax Description

duration *seconds*	Sets the duration of a shun for an attacking host, between 10 and 2592000 seconds. The default length is 3600 seconds (1 hour).
except	Exempts IP addresses from being shunned. Enter this command multiple times to identify multiple IP addresses or network object groups to exempt from shunning.
ip-address *ip_address mask*	Specifies the IP address you want to exempt from shunning.
object-group *network_object_group_id*	Specifies the network object group that you want to exempt from shunning. See the **object-group network** command to create the object group.
shun	Automatically terminates a host connection when the security appliance identifies the host as an attacker, in addition to sending system log message 733101.

Defaults

The default shun duration is 3600 seconds (1 hour).

The following default rate limits are used for scanning attack events:

Table 32-3 Default Rate Limits for Scanning Threat Detection

Average Rate	Burst Rate
5 drops/sec over the last 600 seconds.	10 drops/sec over the last 10 second period.
5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 60 second period.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)/8.1(2)	The **duration** keyword was added.

Usage Guidelines

A typical scanning attack consists of a host that tests the accessibility of every IP address in a subnet (by scanning through many hosts in the subnet or sweeping through many ports in a host or subnet). The scanning threat detection feature determines when a host is performing a scan. Unlike IPS scan detection that is based on traffic signatures, the security appliance scanning threat detection feature maintains an extensive database that contains host statistics that can be analyzed for scanning activity.

The host database tracks suspicious activity such as connections with no return activity, access of closed service ports, vulnerable TCP behaviors such as non-random IPID, and many more behaviors.

Caution The scanning threat detection feature can affect the security appliance performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

You can configure the security appliance to send system log messages about an attacker or you can automatically shun the host. By default, the system log message 733101 is generated when a host is identified as an attacker.

The security appliance identifies attackers and targets when the scanning threat event rate is exceeded. The security appliance tracks two types of rates: the average event rate over an interval, and the burst event rate over a shorter burst interval. For each event detected that is considered to be part of a scanning attack, the security appliance checks the average and burst rate limits. If either rate is exceeded for traffic sent from a host, then that host is considered to be an attacker. If either rate is exceeded for traffic received by a host, then that host is considered to be a target. You can change the rate limits for scanning threat events using the **threat-detection rate scanning-threat** command.

To view hosts categorized as attackers or as targets, use the **show threat-detection scanning-threat** command.

To view shunned hosts, use the **show threat-detection shun** command. To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following example enables scanning threat detection and automatically shuns hosts categorized as attackers, except for hosts on the 10.1.1.0 network. The default rate limits for scanning threat detection are also changed.

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

Related Commands

Command	Description
clear threat-detection shun	Releases a host from being shunned.
show threat-detection scanning-threat	Shows the hosts that are categorized as attackers and targets.

Command	Description
show threat-detection shun	Shows hosts that are currently shunned.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.

threat-detection statistics

To enable scanning threat detection statistics, use the **threat-detection statistics** command in global configuration mode. To disable scanning threat detection statistics, use the **no** form of this command.

Caution Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. The **threat-detection statistics host** command affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. The **threat-detection statistics port** command, however, has modest impact.

threat-detection statistics [**access-list** | **host** [**number-of-rate** {**1** | **2** | **3**} | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

Syntax Description

access-list	(Optional) Enables statistics for access list denies. Access list statistics are only displayed using the **show threat-detection top access-list** command.
average-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the average rate threshold for syslog message generation, between 25 and 2147483647. The default is 200 per second. When the average rate is exceeded, syslog message 733105 is generated.
burst-rate *attacks_per_sec*	(Optional) For TCP Intercept, sets the threshold for syslog message generation, between 25 and 2147483647. The default is 400 per second. When the burst rate is exceeded, syslog message 733104 is generated.
host	(Optional) Enables host statistics. The host statistsics accumulate for as long as the host is active and in the scanning threat host database. The host is deleted from the database (and the statistics cleared) after 10 minutes of inactivity.
number-of-rate {**1** | **2** | **3**}	(Optional) Sets the number of rate intervals maintained for host statistics. Because host statistics use a lot of memory, reducing the number of rate intervals from the default of 3 reduces the memory usage. By default, the **show threat-detection statistics host** command shows information for three rate intervals, for example, for the last 1 hour, 8 hours, and 24 hours. If you set this keyword to 1, then only the shortest rate interval statistics are maintained. If you set the value to 2, then the two shortest intervals are maintained.
port	(Optional) Enables port statistics.
protocol	(Optional) Enables protocol statistics.
rate-interval *minutes*	(Optional) For TCP Intercept, sets the size of the history monitoring window, between 1 and 1440 minutes. The default is 30 minutes. During this interval, the security appliance samples the number of attacks 60 times.
tcp-intercept	(Optional) Enables statistics for attacks intercepted by TCP Intercept. See the **set connection embryonic-conn-max command**, or the **nat** or **static** commands to enable TCP Intercept.

Defaults

Access list statistics are enabled by default. If you do not specify any options in this command, then you enable all options.

The default **tcp-intercept rate-interval** is 30 minutes. The default **burst-rate** is 400 per second. The default **average-rate** is 200 per second.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
8.0(4)/8.1(2)	The **tcp-intercept** keyword was added.
8.1(2)	The **number-of-rates** keyword was added.

Usage Guidelines

View statistics using the **show threat-detection statistics** commands.

You do not need to enable scanning threat detection using the **threat-detection scanning-threat** command; you can configure detection and statistics separately.

Examples

The following example enables scanning threat detection and scanning threat statistics for all types except host:

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection statistics access-list
hostname(config)# threat-detection statistics port
hostname(config)# threat-detection statistics protocol
hostname(config)# threat-detection statistics tcp-intercept
```

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

threshold

To set the threshold value for over threshold events in SLA monitoring operations, use the **threshold** command in SLA monitor configuration mode. To restore the default value, use the **no** form of this command.

threshold *milliseconds*

no threshold

Syntax Description

milliseconds	Specifies the number of milliseconds for a rising threshold to be declared. Valid values are from 0 to 2147483647. This value should not be larger than the value set for the timeout.

Defaults

The default threshold is 5000 milliseconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The threshold value is only used to indicate over threshold events, which do not affect reachability but may be used to evaluate the proper settings for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time the SLA operation waits for a response.

timeout

To set the global maximum idle time duration for various features, use the **timeout** command in global configuration mode. To set all timeouts to the default, use the **no** form of this command. To reset a single feature to its default, reenter the **timeout** command with the default value.

timeout {**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **tcp-proxy-reassembly**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

Syntax Description

absolute	(Optional) Requires a reauthentication after the uauth timeout expires. The **absolute** keyword is enabled by default. To set the uauth timer to timeout after a period of inactivity, enter the **inactivity** keyword instead.
conn	(Optional) Specifies the idle time after which a connection closes, between 0:05:0 and 1193:0:0. The default is 1 hour (1:0:0). Use **0** to never time out a connection.
hh:*mm*:*ss*	Specifies the timeout in hours, minutes, and seconds. Use **0** to never time out a connection, if available.
h225	(Optional) Specifies the idle time after which an H.225 signaling connection closes, between 0:0:0 and 1193:0:0. The default is 1 hour (1:0:0). A timeout value of 0:0:01 disables the timer and closes the TCP connection immediately after all calls are cleared.
h323	(Optional) Specifies the idle time after which H.245 (TCP) and H.323 (UDP) media connections close, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.
half-closed	(Optional) Specifies the idle time after which a TCP half-closed connection will be freed, between 0:5:0 and 1193:0:0. The default is 10 minutes (0:10:0). Use **0** to never time out a connection.
icmp	(Optional) Specifies the idle time for ICMP, between 0:0:02 and 1193:0:0 The default is 2 seconds (0:0:02).
inactivity	(Optional) Requires uauth reauthentication after the inactivity timeout expires.
mgcp	(Optional) Sets the idle time after which an MGCP media connection is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0)
mgcp-pat	(Optional) Sets the absolute interval after which an MGCP PAT translation is removed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0).
rpc	(Optional) Specifies the idle time until an RPC slot is freed, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:05:0).
sip	(Optional) Specifies the dle time after which a SIP control connection will be closed, between 0:5:0 and 1193:0:0. The default is 30 minutes (0:30:0). Use **0** to never time out a connection.

sip-disconnect	(Optional) Specifies the idle time after which a SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 1193:0:0. The default is 2 minutes (0:2:0).
sip-invite	(Optional) Specifies the idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 1193:0:0. The default is 3 minutes (0:3:0).
sip_media	(Optional) Specifies the idle time after which a SIP media connection will be closed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use **0** to never time out a connection. The SIP media timer is used used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
sunrpc	(Optional) Specifies the idle time after which a SUNRPC slot will be closed, between 0:1:0 and 1193:0:0. The default is 10 minutes (0:10:0). Use **0** to never time out a connection.
tcp-proxy-reassembly	(Optional) Configures the idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).
uauth	(Optional) Specifies the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection, between 0:0:0 and 1193:0:0. The default is 5 minutes (0:5:0). The default timer is absolute; you can set the timeout to occur after a period of inactivity by entering the **inactivity** keyword. The **uauth** duration must be shorter than the **xlate** duration. Set to **0** to disable caching. Do not use **0** if passive FTP is used for the connection or if the **virtual http** command is used for web authentication.
udp	(Optional) Specifies the idle time until a UDP slot is freed, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0). Use **0** to never time out a connection.
xlate	(Optional) Specifies the idle time until a translation slot is freed, between 0:1:0 and 1193:0:0. The default is 3 hours (3:0:0).

Defaults

The defaults are as follows:

- **conn** *hh*:*mm*:*ss* is 1 hour (**1:0:0**).
- **h225** *hh*:*mm*:*ss* is 1 hour (**1:0:0**).
- **h323** *hh*:*mm*:*ss* is 5 minutes (**0:5:0**).
- **half-closed** *hh*:*mm*:*ss* is 10 minutes (**0:10:0**).
- **icmp** *hh:mm:ss* is 2 seconds (**0:0:2**)
- **mgcp** *hh:mm:ss* is 5 minutes (**0:5:0**).
- **mgcp-pat** *hh:mm:ss* is 5 minutes (**0:5:0**).
- **rpc** *hh*:*mm*:*ss* is 5 minutes (**0:5:0**).
- **sip** *hh:mm:* is 30 minutes (**0:30:0**).
- **sip-disconnect** *hh:mm:ss* is 2 minutes (**0:2:0**).
- **sip-invite** *hh:mm:ss* is 3 minutes (**0:3:0**).
- **sip_media** *hh:mm:ss* is 2 minutes (**0:2:0**).

- **sunrpc** *hh:mm:ss* is 10 minutes (**0:10:0**)
- **tcp-proxy-reassembly** *hh:mm:ss* is 1 minute (**0:1:0**)
- **uauth** *hh:mm:ss* is 5 minutes (**00:5:00**) **absolute**.
- **udp** *hh*:*mm*:*ss* is 2 minutes (**00:02:00**).
- **xlate** *hh*:*mm*:*ss* is 3 hours (**03:00:00**).

Command Modes

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

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

Command History

Release	Modification
7.2(1)	The **mgcp-pat**, **sip-disconnect**, and **sip-invite** keywords were added.
7.2(5)/8.0(5)/8.1(2)	The **tcp-proxy-reassembly** keyword was added.

Usage Guidelines

The **timeout** command lets you set global timeouts. For some features, the **set connection timeout** command takes precedence for traffic identified in the command.

You can enter multiple keywords and values after the **timeout** command.

The connection timer (**conn**) takes precedence over the translation timer (**xlate**); the translation timer works only after all connections have timed out.

Examples

The following example shows how to configure the maximum idle time durations:

```
hostname(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
hostname(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

Related Commands

Command	Description
clear configure timeout	Clears the timeout configuration and resets it to the defaults.
set connection timeout	Sets connection timeouts using Modular Policy Framework.
show running-config timeout	Displays the timeout value of the designated protocol.

timeout (aaa-server host)

To configure the host-specific maximum response time, in seconds, allowed before giving up on establishing a connection with the AAA server, use the **timeout** command in aaa-server host mode. To remove the timeout value and reset the timeout to the default value of 10 seconds, use the **no** form of this command.

timeout *seconds*

no timeout

Syntax Description

seconds	Specifies the timeout interval (1-60 seconds) for the request. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance sends the request to the backup server.

Defaults

The default timeout value is 10 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is valid for all AAA server protocol types.

Use the **timeout** command to specify the length of time during which the security appliance attempts to make a connection to a AAA server. Use the **retry-interval** command to specify the amount of time the security appliance waits between connection attempts.

The timeout is the total amount of time that the security appliance spends trying to complete a transaction with a server. The retry interval determines how often the communication is retried during the timeout period. Thus, if the retry interval is greater than or equal to the timeout value, you will see no retries. If you want to see retries, the retry interval musts be less than thte timeout value.

Examples

The following example configures a RADIUS AAA server named "svrgrp1" on host 1.2.3.4 to use a timeout value of 30 seconds, with a retry interval of 10 seconds. Thus, the security appliance tries the communication attempt three times before giving up after 30 seconds.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 30
hostname(config-aaa-server-host)# retry-interval 10
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa server host configuration mode so you can configure AAA server parameters that are host specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa	Displays the current AAA configuration values.

timeout (dns-server-group configuration mode)

To specify the amount of time to wait before trying the next DNS server, use the **timeout** command in dns-server-group configuration mode. To restore the default timeout, use the **no** form of this command.

timeout *seconds*

no timeout [*seconds*]

Syntax Description

seconds	Specifies the timeout in seconds between 1 and 30. The default is 2 seconds. Each time the security appliance retries the list of servers, this timeout doubles. Use the **retries** command in dns-server-group configuration mode to configure the number of retries.

Defaults

The default timeout is 2 seconds.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example sets the timeout to 1 second for the DNS server group “dnsgroup1”:

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns timeout 1
```

Related Commands

Command	Description
clear configure dns	Removes all user-created DNS server-groups and resets the default server group’s attributes to the default values.
domain-name	Sets the default domain name.
retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
show running-config dns server-group	Shows the current running DNS server-group configuration.

timeout (gtp-map)

To change the inactivity timers for a GTP session, use the **timeout** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to set these intervals to their default values.

timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

no timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

Syntax Description

hh:*mm*:*ss*	This is the timeout where *hh* specifies the hour, *mm* specifies the minutes, *ss* specifies the seconds, and a colon (:) separates these three components. The value 0 means never tear down immediately.
gsn	Specifies the period of inactivity after which a GSN will be removed.
pdp-context	Specifies the maximum period of time allowed before beginning to receive the PDP context.
request	Specifies the the maximum period of time allowed before beginning to receive the GTP message.
signaling	Specifies the period of inactivity after which the GTP signaling will be removed.
t3-response	Specifies the maximum wait time for a response before a GTP connection is removed.
tunnel	Specifies the period of inactivity after which the GTP tunnel will be torn down.

Defaults

The default is 30 minutes for **gsn**, **pdp-context**, and **signaling**.

The default for **request** is 1 minute.

The default for **tunnel** is 1 hour (in the case where a Delete PDP Context Request is not received).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The Packet Data Protocol (PDP) context is identified by the Tunnel Identifier (TID), which is a combination of IMSI and NSAPI. Each MS can have up to 15 NSAPIs, allowing it to create multiple PDP contexts each with a different NSAPI, based on application requirements for varied QoS levels.

A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station user.

Examples

The following example sets a timeout value for the request queue of 2 minutes:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# timeout request 00:02:00
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

timeout (radius-accounting)

To change the inactivity timers for RADIUS accounting users, use the **timeout** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command. Use the **no** form of this command to set these intervals to their default values.

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

Syntax Description

hh:*mm*:*ss*	This is the timeout where *hh* specifies the hour, *mm* specifies the minutes, *ss* specifies the seconds, and a colon (:) separates these three components. The value 0 means never tear down immediately. The default is one hour.
users	Specifies the timeout for users.

Defaults

The default timeout for users is one hour.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example sets a timeout value for the user of ten minutes:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout user 00:10:00
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

timeout (sla monitor)

To set the amount of time the SLA operation waits for a response to the request packets, use the **timeout** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

timeout *milliseconds*

no timeout

Syntax Description

milliseconds	0 to 604800000.

Defaults

The default timeout value is 5000 milliseconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use the **frequency** command to set how often the SLA operation sends out the request packets and the **timeout** command to set how long the SLA operation waits to receive a response to those requests. The values specified for the **timeout** command cannot be greater than the value specified for the **frequency** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
sla monitor	Defines an SLA monitoring operation.

timeout pinhole

To configure the timeout for DCERPC pinholes and override the global system pinhole timeout of two minutes, use the **timeout pinhole** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

timeout pinhole *hh:mm:ss*

no timeout pinhole

Syntax Description

hh:mm:ss	The timeout for pinhole connections. Value is between 0:0:1 and 1193:0:0.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure the pinhole timeout for pin hole connections in a DCERPC inspection policy map:

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout pinhole 0:10:00
```

Related Commands

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

time-range

To enter time-range configuration mode and define a time range that you can attach to traffic rules, or an action, use the **time-range** command in global configuration mode. To disable, use the **no** form of this command.

time-range *name*

no time-range *name*

Syntax Description

name	Name of the time range. The name must be 64 characters or less.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Creating a time range does not restrict access to the device. The **time-range** command defines the time range only. After a time range is defined, you can attach it to traffic rules or an action.

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

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

Examples

The following example creates a time range named “New_York_Minute” and enters time range configuration mode:

```
hostname(config)# time-range New_York_Minute
hostname(config-time-range)#
```

After you have created a time range and entered time-range configuration mode, you can define time range parameters with the **absolute** and **periodic** commands. To restore default settings for the **time-range** command **absolute** and **periodic** keywords, use the **default** command in time-range configuration mode.

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

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

See the **access-list extended** command for more information about ACLs.

Related Commands

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

timers lsa-group-pacing

To specify the interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** command in router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

Syntax Description

seconds	The interval at which OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged. Valid values are from 10 to 1800 seconds.

Defaults

The default interval is 240 seconds.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To change the interval at which the OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** *seconds* command. To return to the default timer values, use the **no timers lsa-group-pacing** command.

Examples

The following example sets the group processing interval of LSAs to 500 seconds:

```
hostname(config-router)# timers lsa-group-pacing 500
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers spf	Specifies the shortest path first (SPF) calculation delay and hold time

timers spf

To specify the shortest path first (SPF) calculation delay and hold time, use the **timers spf** command in router configuration mode. To restore the default values, use the **no** form of this command.

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

Syntax Description

delay	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds, from 1 to 65535.
holdtime	The hold time between two consecutive SPF calculations in seconds; valid values are from 1 to 65535.

Defaults

The defaults are as follows:

- *delay* is 5 seconds.
- *holdtime* is 10 seconds.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To configure the delay time between when the OSPF protocol receives a topology change and when it starts a calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** command. To return to the default timer values, use the **no timers spf** command.

Examples

The following example sets the SPF calculation delay to 10 seconds and the SPF calculation hold time to 20 seconds:

```
hostname(config-router)# timers spf 10 20
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
timers lsa-group-pacing	Specifies the interval at which OSPF link-state advertisements (LSAs) are collected and refreshed, checksummed, or aged.

title

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

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

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

Syntax Description

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

Defaults

The default title text is “WebVPN Service”.

The default title style is:

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger; vertical-align:middle;text-align:left;font-weight:bold

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

To have no title, use the **title text** command without a *value* argument.

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

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

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

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

Examples

In the following example, the title is customized with the text "Cisco WebVPN Service":

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

Related Commands

Command	Description
logo	Customizes the logo on the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

tls-proxy

To configure a TLS proxy instance in TLS configuration mode or to set the maximum sessions, use the **tls-proxy** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*]

Syntax Description

max_sessions *max_sessions*	Specifies the maximum number of TLS proxy sessions to support on the platform.
proxy_name	Specifies the name of the TLS proxy instance.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **tls-proxy** command to enter TLS proxy configuration mode to create a TLS proxy instance, or to set the maximum sessions supported on the platform.

Be sure to configure the MSS (maximum segment size) value for TCP when using jumbo frames. The MSS should be 120 bytes less than the MTU. For example, if you configure the MTU to be 9000, then the MSS should be configured to 8880. You can configure the MSS with the **sysopt connection tcpmss** command.

Both the primary and the secondary units require a reboot so that the failover pair supports jumbo frames. To avoid downtime, do the following:

- Issue the command on the active unit.
- Save the running configuration on the active unit.
- Reboot the primary and secondary units, one at a time.

Examples

The following example shows how to create a TLS proxy instance:

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.

tos

To define a type of service byte in the IP header of an SLA operation request packet, use the **tos** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

tos *number*

no tos

Syntax Description

number	The service type value to be used in the IP header. Valid values are from 0 to 255.

Defaults

The default type of service value is 0.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This field contains information such as delay, precedence, reliability, and so on. This is can be used by other routers on the network for policy routing and features such as Committed Access Rate.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes, the number of echo requests sent during an SLA operation to 5, and the type of service byte to 80.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# tos 80
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the request packet payload.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

traceroute

To determine the route packets will take to their destination, use the **traceroute** command.

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

Syntax Description

destination_ip	Specifies the destination IP address for the traceroute.
hostname	The hostname of the host to which the route has to be traced. If the hostname is specified, define it with the **name** command, or configure a DNS server to enable traceroute to resolve the hostname to an IP address. Supports DNS domain names such as www.example.com.
source	Specifies an IP address or interface is used as the source for the trace packets.
source_ip	Specifies the source IP address for the packet trace. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the security appliance.
source_interface	Specifies the source interface for the packet trace. When specified, the IP address of the source interface is used.
numeric	Specifies the output print only the IP addresses of the intermediate gateways. If this keyword is not specified the traceroute attempts to look up the hostnames of the gateways reached during the trace.
timeout	Specifies a timeout value is used
timeout_value	Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
probe *probe_num*	The number of probes to be sent at each TTL level. The default count is 3.
ttl	Keyword to specify the range of Time To Live values to use in the probes.
min_ttl	The TTL value for the first probes. The default is 1, but it can be set to a higher value to suppress the display of known hops.
max-ttl	The largest TTL value that can be used. The default is 30. The command terminates when the traceroute packet reaches the destination or when the value is reached.
port *port_value*	The destination port used by the User Datagram Protocol (UDP) probe messages. The default is 33434.
use-icmp	Specifies the use of ICMP probe packets instead of UDP probe packets.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The traceroute command prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the **traceroute** command:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachablee.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Examples

The following example shows traceroute output that results when a destination IP address has been specified:

```
hostname# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

Related Commands

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

track rtr

To track the reachability of an SLA operation, use the **track rtr** command in global configuration mode. To remove the SLA tracking, use the **no** form of this command.

track *track-id* **rtr** *sla-id* **reachabilitity**

no track *track-id* **rtr** *sla-id* **reachabilitity**

Syntax Description

reachability	Specifies that the reachability of the object is being tracked.
sla-id	The ID of the SLA used by the tracking entry.
track-id	Creates a tracking entry object ID. Valid values are from 1 to 500.

Defaults

SLA tracking is disabled.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **track rtr** command creates a tracking entry object ID and specifies the SLA used by that tracking entry.

Every SLA operation maintains an operation return-code value, which is interpreted by the tracking process. The return code may be OK, Over Threshold, or several other return codes. Table 32-4 displays the reachability state of an object with respect to these return codes.

Table 32-4 SLA Tracking Return Codes

Tracking	Return Code	Track State
Reachability	OK or Over Threshold	Up
	Any other code	Down

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

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

```
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
route	Configures a static route.
sla monitor	Defines an SLA monitoring operation.

traffic-non-sip

To allow non-SIP traffic using the well-known SIP signaling port, use the **traffic-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

traffic-non-sip

no traffic-non-sip

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to allow non-SIP traffic using the well-known SIP signaling port in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# traffic-non-sip
```

Related Commands

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

transfer-encoding

To restrict HTTP traffic by specifying a transfer encoding type, use the **transfer-encoding** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of this command.

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a connection using the specified transfer encoding type is detected.
allow	Allows the message.
chunked	Identifies the transfer encoding type in which the message body is transferred as a series of chunks.
compress	Identifies the transfer encoding type in which the message body is transferred using UNIX file compression.
default	Specifies the default action taken by the security appliance when the traffic contains a supported request method that is not on a configured list.
deflate	Identifies the transfer encoding type in which the message body is transferred using zlib format (RFC 1950) and deflate compression (RFC 1951).
drop	Closes the connection.
gzip	Identifies the transfer encoding type in which the message body is transferred using GNU zip (RFC 1952).
identity	Identifies connections in which the message body is no transfer encoding is performed.
log	(Optional) Generates a syslog.
reset	Sends a TCP reset message to client and server.
type	Specifies the type of transfer encoding to be controlled through HTTP application inspection.

Defaults

This command is disabled by default. When the command is enabled and a supported transfer encoding type is not specified, the default action is to allow the connection without logging. To change the default action, use the **default** keyword and specify a different default action.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you enable the **transfer-encoding** command, the security appliance applies the specified action to HTTP connections for each supported and configured transfer encoding type.

The security appliance applies the **default** action to all traffic that does *not* match the transfer encoding types on the configured list. The preconfigured **default** action is to **allow** connections without logging.

For example, given the preconfigured default action, if you specify one or more encoding types with the action of **drop** and **log**, the security appliance drops connections containing the configured encoding types, logs each connection, and allows all connections for the other supported encoding types.

If you want to configure a more restrictive policy, change the default action to **drop** (or **reset**) and **log** (if you want to log the event). Then configure each permitted encoding type with the **allow** action.

Enter the **transfer-encoding** command once for each setting you wish to apply. You use one instance of the **transfer-encoding** command to change the default action and one instance to add each encoding type to the list of configured transfer encoding types.

When you use the **no** form of this command to remove an application category from the list of configured application types, any characters in the command line after the application category keyword are ignored.

Examples

The following example provides a permissive policy, using the preconfigured default, which allows all supported application types that are not specifically prohibited.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# transfer-encoding gzip drop log
hostname(config-http-map)#
```

In this case, only connections using GNU zip are dropped and the event is logged.

The following example provides a restrictive policy, with the default action changed to reset the connection and to log the event for any encoding type that is not specifically allowed.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse identity allow
hostname(config-http-map)#
```

In this case, only connections using no transfer encoding are allowed. When HTTP traffic for the other supported encoding types is received, the security appliance resets the connection and creates a syslog entry.

Related Commands

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

trust-point

To specify the name of a trustpoint that identifies the certificate to be sent to the IKE peer, use the **trust-point** command in tunnel-group ipsec-attributes mode. To eliminate a trustpoint specification, use the **no** form of this command.

trust-point *trust-point-name*

no trust-point *trust-point-name*

Syntax Description

trust-point-name	Specifies the name of the trustpoint to use.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example entered in config-ipsec configuration mode, configures a trustpoint for identifying the certificate to be sent to the IKE peer for the IPSec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
```

Related Commands

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

trustpoint (SSO Server)

To specify the name of a trustpoint that identifies the certificate to be sent to the SAML POST-type SSO server, use the **trustpoint** command in config-webvpn-sso-saml mode. To eliminate a trustpoint specification, use the **no** form of this command.

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	Specifies the name of the trustpoint to use.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Config webvpn sso saml	•	—	•	—	—

Command History

Release	Modification
7.3	This command is introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The security appliance currently supports the SAML POST-type SSO server and the SiteMinder-type of SSO server.

This command applies only to SAML-type SSO Servers.

A trustpoint represents a Certificate Authority identity, based on a CA-issued certificate that can be relied upon as being valid without the need for validation testing, especially a public-key certificate used to provide the first public key in a certification path.

Examples

The following example enters config-webvpn-sso-saml mode and names a trustpoint for identifying the certificate to be sent to the SAML POST type SSO Server:

```
hostname(config-webvpn)# sso server
hostname(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

Related Commands

Command	Description
crypto ca trustpoint	Manages trustpoint information.
show webvpn sso server	Displays the operating statistics for all SSO servers configured on the security device.
sso server	Creates, names, and specifies type for an SSO server.

tsig enforced

To require a TSIG resource record to be present, use the **tsig enforced** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

Syntax Description

drop	Drops the packet if TSIG is not present.
log	Generates a system message log.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command enables monitoring and enforcement of TSIG presence in DNS transactions.

Examples

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

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tsig enforced action log
```

Related Commands

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

ttl-evasion-protection

To disable the Time-To-Live evasion protection, use the **ttl-evasion-protection** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

ttl-evasion-protection

no ttl-evasion-protection

Syntax Description

This command has no arguments or keywords.

Defaults

TTL evasion protection offered by the security appliance is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **ttl-evasion-protection** command in tcp-map configuration mode to prevent attacks that attempt to evade security policy.

For instance, an attacker can send a packet that passes policy with a very short TTL. When the TTL goes to zero, a router between the security appliance and the endpoint drops the packet. It is at this point that the attacker can send a malicious packet with a long TTL that appears to the security appliance to be a retransmission and is passed. To the endpoint host, however, it is the first packet that has been received by the attacker. In this case, an attacker is able to succeed without security preventing the attack. Enabling this feature prevents such attacks.

Examples

The following example shows how to disable TTL evasion protection on flows from network 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# ttl-evasion-protection disable
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

tunnel-group

To create and manage the database of connection-specific records for IPSec and WebVPN tunnels, use the **tunnel-group** command in global configuration mode. To remove a tunnel group, use the **no** form of this command.

tunnel-group *name* **type** *type*

no tunnel-group *name*

Syntax Description

name	Specifies the name of the tunnel group. This can be any string you choose. If the name is an IP address, it is usually the IP address of the peer.
type	Specifies the type of tunnel group: • remote-access—Allows a user to connect using either IPSec remote access or WebVPN (portal or tunnel client). • ipsec-l2l—Specifies IPsec LAN-to-LAN, which allows two sites or LANs to connect securely across a public network like the Internet. **Note** The following tunnel-group types are deprecated in Release 8.0(2): ipsec-ra—IPSec remote access webvpn—WebVPN The security appliance converts these to the remote-access type.

Defaults

No default behavior or values.

Command Modes

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

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

Note The tunnel-group command is available in transparent firewall mode to allow configuration of a LAN-to-LAN tunnel group, but not a remote-access group or a WebVPN group. All the tunnel-group commands that are available for LAN-to-LAN are also available in transparent firewall mode.

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added webvpn type.
8.0(2)	Added remote-access type and deprecated ipsec-ra and webvpn types.

Usage Guidelines

The security appliance has the following default tunnel groups:

- DefaultRAGroup, the default IPSec remote-access tunnel group
- DefaultL2LGroup, the default IPSec LAN-to-LAN tunnel group
- DefaultWEBVPNGroup, the default WebVPN tunnel group.

You can change these groups, but not delete them. The security appliance uses these groups to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

After entering the **tunnel-group** command, you enter the appropriate following commands to configure specific attributes for a particular tunnel group. Each of these commands enters a configuration mode for configuring tunnel-group attributes.

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

Examples

The following examples are entered in global configuration mode. The first configures a remote access tunnel group. The group name is group1.

```
hostname(config)# tunnel-group group1 type remote-access
hostname(config)#
```

The following example shows the tunnel-group command configuring the webvpn tunnel group named "group1". You enter this command in global configuration mode:

```
hostname(config)# tunnel-group group1 type webvpn
hostname(config)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Enters the config-general mode for configuring general tunnel-group attributes
tunnel-group ipsec-attributes	Enters the config-ipsec mode for configuring IPSec tunnel-group attributes.
tunnel-group ppp-attributes	Enters the config-ppp mode for configuring PPP settings for L2TP connections.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

tunnel-group general-attributes

To enter the general-attribute configuration mode, use the **tunnel-group general-attributes** command in global configuration mode. This mode is used to configure settings that are common to all supported tunneling protocols.

To remove all general attributes, use the **no** form of this command.

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

Syntax Description

general-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Various attributes from other tunnel-group types migrated to the general tunnel-group attributes list, and the prompt for tunnel-group general-attributes mode changed.

Examples

The following example entered in global configuration mode, creates a remote-access tunnel group for a remote-access connection using the IP address of the LAN-to-LAN peer, then enters general-attributes configuration mode for configuring tunnel-group general attributes. The name of the tunnel group is 209.165.200.225.

```
hostname(config)# tunnel-group 209.165.200.225 type remote-access
hostname(config)# tunnel-group 209.165.200.225 general-attributes
hostname(config-tunnel-general)#
```

The following example entered in global configuration mode, creates a tunnel group named” remotegrp” for an IPSec remote access connection, and then enters general configuration mode for configuring general attributes for the tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
```

```
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group ipsec-attributes

To enter the ipsec-attribute configuration mode, use the **tunnel-group ipsec-attributes** command in global configuration mode. This mode is used to configure settings that are specific to the IPSec tunneling protocol.

To remove all IPSec attributes, use the **no** form of this command.

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

Syntax Description

ipsec-attributes	Specifies attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Various IPSec tunnel-group attributes migrated to the general tunnel-group attributes list, and the prompt for tunnel-group ipsec-attributes mode changed.

Examples

The following example entered in global configuration, creates a tunnel group for the IPSec remote-access tunnel group named remotegrp, and then specifies IPSec group attributes:

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

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group ppp-attributes

To enter the ppp-attributes configuration mode and configure PPP settings that are used by L2TP over IPSec connections, use the **tunnel-group ppp-attributes** command in global configuration mode.

To remove all PPP attributes, use the **no** form of this command.

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

Syntax Description

name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

PPP settings are used by the Layer 2 Tunneling Protocol (L2TP), a VPN tunneling protocol which allows remote clients to use the dialup telephone service public IP network to securely communicate with private corporate network servers. L2TP is based on the client/server model and uses PPP over UDP (port 1701) to tunnel the data. All of the tunnel-group ppp commands are available for the PPPoE tunnel-group type.

Examples

The following example creates the tunnel group *telecommuters* and enters ppp-attributes configuration mode:

```
hostname(config)# tunnel-group telecommuters type pppoe
hostname(config)# tunnel-group telecommuters ppp-attributes
hostname(tunnel-group-ppp)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.

Command	Description
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group webvpn-attributes

To enter the webvpn-attribute configuration mode, use the **tunnel-group webvpn-attributes** command in global configuration mode. This mode configures settings that are common to WebVPN tunneling.

To remove all WebVPN attributes, use the **no** form of this command.

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

Syntax Description

webvpn-attributes	Specifies WebVPN attributes for this tunnel-group.
name	Specifies the name of the tunnel-group.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

The following example entered in global configuration mode, creates a tunnel group for a WebVPN connection using the IP address of the LAN-to-LAN peer, then enters webvpn-configuration mode for configuring WebVPN attributes. The name of the tunnel group is 209.165.200.225.

```
hostname(config)# tunnel-group 209.165.200.225 type webvpn
hostname(config)# tunnel-group 209.165.200.225 webvpn-attributes
hostname(config-tunnel-webvpn)#
```

The following example entered in global configuration mode, creates a tunnel group named" remotegrp" for a WebVPN connection, and then enters webvpn configuration mode for configuring WebVPN attributes for the tunnel group named "remotegrp":

```
hostname(config)# tunnel-group remotegrp type webvpn
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears the entire tunnel-group database or just the specified tunnel-group.
show running-config tunnel-group	Displays the currently running tunnel-group configuration for a specified tunnel group or for all tunnel groups.
tunnel-group	Creates and manages the database of connection-specific records for IPSec and WebVPN tunnels.

tunnel-group-map default-group

The **tunnel-group-map default-group** command specifies the default tunnel-group to use if the name could not be determined using other configured methods.

Use the **no** form of this command to eliminate a tunnel-group-map.

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

Syntax Description

default-group *tunnel-group-name*	Specifies a default tunnel group to use when the name cannot be derived by other configured methods. The *tunnel-group name* must already exist.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Defaults

The default value for the **tunnel-group-map default-group** is DefaultRAGroup.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The tunnel-group-map commands configure the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. To associate the certificate map entries, created using the **crypto ca certificate map** command, with tunnel groups, use the **tunnel-group-map** command in global configuration mode. You can invoke this command multiple times as long as each invocation is unique and you do not reference a map index more than once.

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

The processing that derives the tunnel-group name from the certificate ignores entries in the certificate map that are not associated with a tunnel group (any map rule not identified by this command).

Examples

The following example entered in global configuration mode, specifies a default tunnel group to use when the name cannot be derived by other configured methods. The name of the tunnel group to use is group1:

```
hostname(config)# tunnel-group-map default-group group1
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters crypto ca certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map enable	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups

tunnel-group-map enable

The **tunnel-group-map enable** command configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups. Use the **no** form of this command to restore the default values.

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

Syntax Description

policy	Specifies the policy for deriving the tunnel group name from the certificate. *Policy* can be one of the following: **ike-id**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou, then the certificate-based IKE sessions are mapped to a tunnel group based on the content of the phase1 IKE ID. **ou**—Indicates that if a tunnel-group is not determined based on a rule lookup, then use the value of the organizational unit (OU) in the subject distinguished name (DN). **peer-ip**—Indicates that if a tunnel-group is not determined based on a rule lookup or taken from the ou or ike-id methods, then use the established peer IP address. **rules**—Indicates that the certificate-based IKE sessions are mapped to a tunnel group based on the certificate map associations configured by this command.
rule index	Optional. Refers to parameters specified by the **crypto ca certificate map** command. The values are 1 to 65535.

Defaults

The default values for the **tunnel-group-map** command are **enable ou** and **default-group** set to DefaultRAGroup.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **crypto ca certificate map** command maintains a prioritized list of certificate mapping rules. There can be only one map. But this map can have up to 65535 rules. Refer to the documentation on the **crypto ca certificate map** command for more information.

Examples

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the content of the phase1 IKE ID:

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions to a tunnel group based on the established IP address of the peer:

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions based on the organizational unit (OU) in the subject distinguished name (DN):

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

The following example enables mapping of certificate-based IKE sessions based on established rules:

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map default-group	Designates an existing tunnel-group name as the default tunnel group.

tunnel-limit

To specify the maximum number of GTP tunnels allowed to be active on the security appliance, use the **tunnel limit** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** to set the tunnel limit back to its default.

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

Syntax Description

max_tunnels	This is the maximum number of tunnels allowed. The ranges is from 1 to 4294967295 for the global overall tunnel limit.

Defaults

The default for the tunnel limit is 500.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

New requests will be dropped once the number of tunnels specified by this command is reached.

Examples

The following example specifies a maximum of 10,000 tunnels for GTP traffic:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.

Commands	Description
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

tx-ring-limit

To specify the depth of the priority queues, use the **tx-ring-limit** command in priority-queue mode. To remove this specification, use the **no** form of this command.

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears. The upper limit of the range of values is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device.

Defaults

The default **tx-ring-limit** is 128 packets.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The security appliance recognizes priority traffic and enforces appropriate Quality of Service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.

You must use the **priority-queue** command to create the priority queue for an interface before priority queuing takes effect. You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue mode, as shown by the prompt. In priority-queue mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best -effort) allowed to be buffered before dropping packets (**queue-limit** command).

Note You *must* configure the **priority-queue** command in order to enable priority queueing for the interface.

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop*. To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 240 packets and a transmit queue limit of 3 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 240
hostname(priority-queue)# tx-ring-limit 3
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current **priority-queue**, **queue-limit**, and **tx-ring-limit** command configuration values.

type echo

To configure the SLA operation as an echo response time probe operation, use the **type echo** command in SLA monitor configuration mode. To remove the type from teh SLA configuration, use the **no** form of this command.

type echo protocol ipIcmpEcho *target* interface *if-name*

no type echoprotocol ipIcmpEcho *target* interface *if-name*

Syntax Description

interface *if-name*	Specifies the interface name, as specified by the **nameif** command, of the interface used to send the echo request packets. The interface source address is used as the source address in the echo request packets.
protocol	The protocol keyword. The only value supported is **ipIcmpEcho**, which specifies using an IP/ICMP echo request for the echo operation.
target	The IP address or host name of the object being monitored.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The default size of the payload of the ICMP packets is 28 bytes, creating a total ICMP packet size of 64 bytes. The payload size can be changed using the **request-data-size** command.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 10 seconds, the threshold to 2500 milliseconds, and the timeout value us set to 4000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
request-data-size	Specifies the size of the payload for the SLA operation request packet.
sla monitor	Defines an SLA monitoring operation.