CHAPTER 32

tcp-map through tx-ring-limit 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
hostname(config)#
```

Related Commands

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

telnet

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

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

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

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

```
hostname# passwd: cisco

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

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

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

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

Related Commands

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

terminal

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

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

Syntax Description

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

Defaults

System log messages are disabled by default.

Command Modes

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

	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 logging and then disable logging only in the current session:

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

Related Commands

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

terminal pager

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

terminal pager [lines] *lines*

Syntax Description

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

Defaults

The default is 24 lines.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

```
hostname# terminal pager 20
```

Related Commands

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

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

terminal width

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

terminal width *columns*

no terminal width *columns*

Syntax Description

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

Defaults

The default display width is 80 columns.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

```
hostname# terminal width 100
```

Related Commands

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

test aaa-server

Use the **test aaa-server** command to check whether the security appliance can authenticate or authorize users with a particular AAA server. 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 | authorization} *server-tag* **[host** *server-ip*] **[username** *username*] **[password** *password*]

Syntax Description

authentication	Specifies that the security appliance should send a test authentication request.
authorization	Specifies that the security appliance should send a test authorization request.
host *server-ip*	Specifies The IP address of the AAA server.
password *password*	Specifies the password for the username given. The **password** argument is available only for authentication tests. Make sure the password is correct for the username entered; otherwise, the authentication test will fail.
server-tag	Specifies the symbolic name of the server group, as defined by the **aaa-server protocol** 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **test aaa-server** command enables you to verify that the security appliance can authenticate and authorize users with a particular AAA server. Using this command simplifies verification of the configuration on the security appliance by removing the necessity of testing with a real supplicant. It also helps you isolate whether authentication and authorization failures are due to misconfiguration of AAA server parameters, a connection problem to the AAA server, or other configuration errors on the security appliance.

When you enter the command, you can omit the **host** and **password** keyword and argument pairs. The security appliance will prompt you for their values. If you are performing an authentication test, you can also omit the **password** keyword and argument pair and provide the password when the security appliance prompts you.

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: ******
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Server not responding: No error
```

Related Commands

Command	Description
aaa-server host	Specifies parameters for a specific AAA server.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

test sso-server

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

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
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 reentering 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.

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 Anyuser is not recognized and the authentication fails:

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

```
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 an SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SSO authentication requests.

text-color

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

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

no text-color

Syntax Description

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

Defaults

The default text color for the title bars is white.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

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

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

Related Commands

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

tftp-server

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

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

Syntax Description

interface_name	Specifies the gateway interface name. If you specify an interface other than the highest security interface, a warning message informs you that the interface is unsecure.
server	Sets the TFTP server IP address or name. You can enter an IPv4 or IPv6 address.
filename	Specifies the path and filename.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

timeout

To set the maximum idle time duration, use the **timeout** command in global configuration mode.

timeout [**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip_media** | **uauth** *hh*:*mm*:*ss*]

Syntax Description

conn	(Optional) Specifies the idle time after which a connection closes; the minimum duration is five minutes.
hh:*mm*:*ss*	Specifies the timeout.
h225 *hh*:*mm*:*ss*	(Optional) Specifies the idle time after which an H.225 signaling connection closes.
h323	(Optional) Specifies the idle time after which H.245 (TCP) and H.323 (UDP) media connections close. The default is five minutes. **Note** Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.
half-closed	(Optional) Specifies the idle time after which a TCP half-closed connection will be freed.
icmp	(Optional) Specifies the idle time for ICMP.
mgcp *hh:mm:ss*	(Optional) Sets the idle time after which an MGCP media connection is removed.
mgcp-pat *hh:mm:ss*	(Optional) Sets the absolute interval after which an MGCP PAT translation is removed.
rpc	(Optional) Specifies the idle time until an RPC slot is freed; the minimum duration is one minute.
sip	(Optional) Modifies the SIP timer.
sip_media	(Optional) Modifies the SIP media timer, which is 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.
uauth	(Optional) Sets the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection.
udp	(Optional) Specifies the idle time until a UDP slot is freed; the minimum duration is one minute.
xlate	(Optional) Specifies the idle time until a translation slot is freed; the minimum value is one minute.

Defaults

The defaults are as follows:

- **conn** *hh*:*mm*:*ss* is 1 hour (**01:00:00**).
- **h225** *hh*:*mm*:*ss* is 1 hour (**01:00:00**).
- **h323** *hh*:*mm*:*ss* is 5 minutes (**00:05:00**).
- **half-closed** *hh*:*mm*:*ss* is 10 minutes (**00:10:00**).

- **icmp** *hh:mm:ss* is 2 minutes (**00:00:0***2*)
- **mgcp** *hh:mm:ss* is 5 minutes (**00:05:00**).
- **mgcp-pat** *hh:mm:ss* is 5 minutes (**00:05:00**).
- **rpc** *hh*:*mm*:*ss* is 10 minutes (**00:10:00**).
- **sip** *hh:mm:* is 30 minutes (**00:30:00**).
- **sip_media** *hh:mm:ss* is 2 minutes (**00:02:00**).
- **sunrpc** *hh:mm:ss* is 10 minutes (**00:10:00**)
- **uauth** timer is **absolute**.
- **udp** *hh*:*mm*:*ss* is 2 minutes (**00:02:00**).
- **xlate** *hh*:*mm*:*ss* is 3 hours (**03:00:00**).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	They keyword **mgcp-pat** was added.

Usage Guidelines

The **timeout** command lets you set the idle time for connection, translation UDP, and RPC slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

Note Do not use the **timeout uauth 0:0:0** command if passive FTP is used for the connection or if the **virtual** command is used for web authentication.

The connection timer takes precedence over the translation timer; the translation timer works only after all connections have timed out.

When setting the **conn** *hh*:*mm*:*ss*, use **0:0:0** to never time out a connection.

When setting the **half-closed** *hh*:*mm*:*ss*, use **0:0:0** to never time out a half-closed connection.

When setting the **h255** *hh*:*mm*:*ss*, **h225 00:00:00** means to never tear down an H.225 signaling connection. A timeout value of **h225 00:00:01** disables the timer and closes the TCP connection immediately after all calls are cleared.

The **uauth** *hh*:*mm*:*ss* duration must be shorter than the **xlate** keyword. Set to **0** to disable caching. Do not set to zero if passive FTP is used on the connections.

To disable the **absolute** keyword, set the uauth timer to 0 (zero).

Examples

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

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

Related Commands

Command	Description
show running-config timeout	Displays the timeout value of the designated protocol.

timeout (aaa-server host)

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

timeout *seconds*

no timeout

Syntax Description

seconds	Specifies the timeout interval (1-60 seconds) for the request. This is the time after which the 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 (gtp-map)

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

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

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

Syntax Description

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.
tunnel	Specifies the the period of inactivity after which the GTP tunnel will be torn down.

Defaults

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

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

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

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	No

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The 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 (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. **Reviewers: This was true for the dns timeout and retries commands. Is it also true for the timeout command in dns-server-group configuration mode?**

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	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.

Command	Description
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.

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":

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(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.

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
hostname(config-tunnel-ipsec)#
```

Related Commands

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

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: ipsec-ra—IPSec remote access ipsec-l2l—IPsec LAN-to-LAN webvpn—WebVPN

Defaults

No default behavior or values.

Command Modes

The following table 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	This command was introduced.
7.1	Added webvpn type.

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**

Examples

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

```
hostname(config)# tunnel-group group1 type ipsec-ra
hostname(config)#
```

The following example configures an IPSec LAN-to-LAN tunnel group. The name is the IP address of the LAN-to-LAN peer:

```
hostname(config)# tunnel-group 209.165.200.225 type ipsec-l2l
hostname(config)#
```

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 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**
Global 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.

Usage Guidelines

The following table lists the commands belonging in this group and the tunnel-group type where you can configure them:

General Attribute	Availability by Tunnel-Group Type
accounting-server-group	IPSec RA, IPSec L2L, WebVPN
address-pool	IPSec RA
authentication-server-group	IPSec RA, WebVPN
authorization-dn-attributes	IPSec RA, WebVPN
authorization-required	WebVPN
authorization-server-group	IPSec RA

General Attribute	Availability by Tunnel-Group Type
default-group-policy	IPSec RA, IPSec L2L
dhcp-server	IPSec RA
override-account-disabled	IPSec RA, WebVPN
password-management	IPSec RA, WebVPN
strip-group	IPSec RA, WebVPN,
strip-realm	IPSec RA, WebVPN

Examples

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

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 general
hostname(config-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.

Usage Guidelines

The following commands belong in this group:

IPSec Attribute	Availability by Tunnel-Group Type
chain	IPSec RA, IPSec L2L
client-update	IPSec RA
isakmp keepalive	IPSec RA
peer-id-validate	IPSec RA, IPSec L2L
pre-shared-key	IPSec RA, IPSec L2L
radius-with-expiry	IPSec RA
trust-point	IPSec RA, IPSec L2L

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.
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.

Usage Guidelines

In addition to the general attributes, you can also configure the following attributes specific to WebVPN connections in webvpn-attribute mode:

- authentication
- customization
- dns-group
- group-alias
- group-url
- hic-fail-group-policy
- nbns-server-name

See the individual command descriptions for complete information about configuring these attributes.

Examples

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

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

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

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

Related commands

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

tunnel-group-map default-group

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

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

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

no tunnel-group-map

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

tunnel-group-map enable

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

tunnel-limit

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

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

Syntax Description

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

Defaults

The default for the tunnel limit is 500.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

tx-ring-limit

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

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

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

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets allowed into the Ethernet transmit driver before the driver pushes back to the queues on the interface to let them buffer packets until the congestion clears. The range of **tx-ring-limit** values is 3 through 128 packets on the PIX platform and 3 through 256 packets on the ASA platform.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

Note The upper limit of the range of values for the **queue-limit** and **tx-ring-limit** commands is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device. The range of **queue-limit** values is 0 through 2048 packets. The range of **tx-ring-limit** values is 3 through 128 packets on the PIX platform and 3 through 256 packets on the ASA platform.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 2048 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 2048
hostname(priority-queue)# tx-ring-limit 256
```

Related Commands

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