ta – tk

table-map

To modify metric and tag values when the IP routing table is updated with BGP learned routes, use the **table-map** command in address family configuration mode. To disable this function, use the **no** form of the command.

table-map *map_name* [**filter**]
no table-map *map_name* [**filter**]

Syntax Description

map_name	The name of the route map that should control what gets put into the BGP routing table (RIB).
filter	(Optional) Specifies that the route map controls not only the metrics on a BGP route, but also whether the route is downloaded into the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

Command Default

This command is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

A table map references a route map that sets metrics and a tag value for routes that are updated in the BGP routing table, or controls whether routes are downloaded to the RIB.

When the table-map command:

- Does not include the **filter** keyword, the route map referenced is used to set certain properties of a route before the route is installed (downloaded) into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- Includes the **filter** keyword, the route map referenced also controls whether the BGP route is downloaded to the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

You can use match clauses in the route map that the table map references to match routes based on IP access list, autonomous system paths, and next hop.

Examples

In the following address family configuration mode example, the Secure Firewall ASA software is configured to automatically compute the tag value for the BGP learned routes and to update the IP routing table:

```
ciscoasa(config)# route-map tag
ciscoasa(config-route-map)# match as path 10
ciscoasa(config-route-map)# set automatic-tag
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# table-map tag
```

Related Commands

Command	Description
address-family	Enters the address-family configuration mode.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

tcp-inspection

To enable DNS over TCP inspection, use the **tcp-inspection** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

tcp-inspection
no tcp-inspection

Syntax Description

This command has no arguments or keywords.

Command Default

DNS over TCP inspection is disabled.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Add this command to a DNS inspection policy map to include DNS/TCP port 53 traffic in the inspection. Without this command, UDP/53 DNS traffic only is inspected. Ensure that DNS/TCP port 53 traffic is part of the class to which you apply DNS inspection. The inspection default class includes TCP/53.

Examples

The following example shows how to enable DNS over TCP inspection a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# tcp-inspection
```

Related Commands

Command	Description
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
show running-config policy-map	Display all current policy map configurations.

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 ASA 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)/8.0(4)	The **invalid-ack**, **seq-past-window**, and **synack-data** subcommands were added.

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 CLI 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.
invalid-ack	Sets the action for packets with an invalid ACK.

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 ASA. On the PIX 500 series ASA, the queue limit is 3 and cannot be changed.
reserved-bits	Sets the reserved flags policy in the ASA.
seq-past-window	Sets the action for packets that have past-window sequence numbers, namely the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window.
synack-data	Sets the action for TCP SYNACK packets that contain data.
syn-data	Allows or drops SYN packets with data.
tcp-options	Sets the action for packets based on the contents of the TCP options field in the TCP header.
ttl-evasion-protection	Enables or disables the TTL evasion protection offered by the ASA.
urgent-flag	Allows or clears the URG pointer through the ASA.
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:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config-tcp-map)# class-map urg-class
ciscoasa(config-cmap)# match port tcp range ftp-data telnet
ciscoasa(config-cmap)# policy-map pmap
ciscoasa(config-pmap)# class urg-class
ciscoasa(config-pmap-c)# set connection advanced-options tmap
ciscoasa(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 in a TCP header, use the **tcp-options** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

tcp-options { **md5 | mss | selective-ack | timestamp | window-scale | range** *lower upper* } *action*
no tcp-options { **md5 | mss | selective-ack | timestamp | window-scale | range** *lower upper* } *action*

Syntax Description

action	The action to perform for the option. Actions are: • **allow** [**multiple**]—Allow packets that contain the option. Starting with 9.6(2), **allow** means to allow packets that contain a single option of this type. This is the default for all of the named options. If you want to allow packets even if they contain more than one instance of the option, add the **multiple** keyword. The **multiple** keyword is not available with **range**. • **maximum** *limit*—For **mss** only. Set the maximum segment size to the indicated limit, from 68-65535. The default TCP MSS is defined on the **sysopt connection tcpmss** command. • **clear**—Remove the options of this type from the header and allow the packet. This is the default for all of the numbered options you can configure on the **range** keyword. Note that clearing the timestamp option disables PAWS and RTT. • **drop**—Drop packets that contain this option. This action is available for **md5** and **range** only.
md5	Sets the action for the MD5 option.
mss	Sets the action for the maximum segment size option.
range *lower upper*	Sets with action for the numbered options within the lower and upper bounds of the range. To set the action for a single numbered option, enter the same number for the lower and upper range. (9.6(2) and later.) The valid ranges are within 6-7, 9-18, and 20-255. (9.6(1) and earlier.) The valid ranges are within 6-7 and 9-255.
selective-ack	Sets the action for the selective acknowledgment mechanism (SACK) option.
timestamp	Sets the action for the timestamp option. Clearing the timestamp option will disable PAWS and RTT.
window-scale	Sets the action for the window scale mechanism option.

Command Default

(9.6(1) and earlier.) The default is to allow all of the named options, and clear options 6-7 and 9-255.

(9.6(2) and later.) The default is to allow a single instance of each of the named options, drop packets with more than one of a given named option, and clear options 6-7, 9-18, and 20-155.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.6(2)	Default handling of the named options was changed to allow a packet if it contains a single option of a given type, and drop the packet if there are more than one option of that type. Also, the **md5**, **mss**, **allow multiple**, and **mss maximum** keywords were added. The default for the MD5 option was changed from clear to allow.

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 define how the various TCP options should be handled.

Examples

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

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# tcp-options range 6 7 drop
ciscoasa(config-tcp-map)# tcp-options range 9 18 drop
ciscoasa(config-tcp-map)# tcp-options range 20 255 drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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 allow Telnet access to an interface, use the **telnet** command in global configuration mode. To remove Telnet access, use the **no** form of this command.

telnet { *ipv4_address mask* | *ipv6_address/prefix* } *interface_name*
no telnet { *ipv4_address mask* | *ipv6_address/prefix* } *interface_name*

Syntax Description

interface_name	Specifies the name of the interface on which to allow Telnet. You cannot enable Telnet on the lowest security interface unless you use Telnet in a VPN tunnel. A physical or virtual interface can be specified.
ipv4_address mask	Specifies the IPv4 address of a host or network authorized to Telnet to the ASA, and the subnet mask.
ipv6_address/prefix	Specifies the IPv6 address/prefix authorized to Telnet to the ASA.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(2), 9.1(2)	The default password, “cisco” has been removed; you must actively set a login password using the **password** command.
9.9.(2)	Virtual interfaces can now be specified.

Usage Guidelines

The **telnet** command lets you specify which hosts can access the ASA CLI with Telnet. You can enable Telnet to the ASA on all interfaces. However, You cannot use Telnet to the lowest security interface unless you use Telnet inside a VPN tunnel. Also, if a BVI interface is specified, managenent-access must be configured on that interface.

Use the password command to set a password for Telnet access to the console. Use the who command to view which IP addresses are currently accessing the ASA console. Use the kill command to terminate an active Telnet console session.

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

Examples

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

```
ciscoasa(config)# telnet 192.168.1.3 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.1.4 255.255.255.255 inside
ciscoasa(config)# telnet 192.168.2.0 255.255.255.0 inside
ciscoasa(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 a Telnet console login session (the password does not display when entered):

```
ciscoasa# passwd: cisco
Welcome to the XXX
…
Type help or '?' for a list of available commands.
ciscoasa>
```

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

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

ciscoasa(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 ASA.
telnet timeout	Sets the Telnet timeout.
who	Displays active Telnet administration sessions on the ASA.

telnet timeout

To set the Telnet idle timeout, use the **telnet timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

telnet timeout *minutes*
no telnet timeout *minutes*

Syntax Description

minutes	Number of minutes that a Telnet session can be idle before being closed by the ASA. Valid values are from 1 to 1440 minutes. The default is 5 minutes.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the telnet timeout command to set the maximum time that a console Telnet session can be idle before being logged off by the ASA.

Examples

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

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

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 ASA.
telnet	Enables Telnet access to the ASA.

Command	Description
who	Displays active Telnet administration sessions on the ASA.

terminal interactive

To enable help in the current CLI session when you enter **?** at the CLI, use the **terminal interactive** command in privileged EXEC mode. To disable CLI help, use the **no** form of this command.

terminal interactive
no terminal interactive

Syntax Description

This command has no arguments or keywords.

Command Default

Interactive CLI help is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Normally, when you enter **?** at the ASA CLI, you see command help. To be able to enter **?** as text within a command (for example, to include a **?** as part of a URL), you can disable interactive help using the **no terminal interactive** command.

Examples

The following example shows how to turn the console into a non-interactive mode, then into an interactive mode:

```
ciscoasa# no
 terminal interactive
ciscoasa# terminal interactive
```

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.

Command	Description
terminal width	Sets the terminal display width in global configuration mode.

terminal monitor

To allow syslog messages to show in the current CLI session, use the **terminal monitor** command in privileged EXEC mode. To disable syslog messages, use the **no** form of this command.

terminal { **monitor | no monitor** }

Syntax Description

monitor	Enables the display of syslog messages in the current CLI session.
no monitor	Disables the display of syslog messages in the current CLI session.

Command Default

Syslog messages are disabled by default. This command is interactive by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to display and disable syslog messages in the current session:

```
ciscoasa# terminal monitor
ciscoasa# 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.

Command Default

The default is 24 lines.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command changes the pager line setting only for the current Telnet session. However, the ASA re-initiates the pager value in the current session from the running-config only when you enter the **login** command in user EXEC mode or enter the **enable** command to enter privileged EXEC mode. This is as-designed.

Note An unexpected "--- More---" prompt occurs before the ASA redisplays the user prompt, which may have suppressed the output of the **banner exec** command. Use the **banner motd** command or **banner login** command instead.

To save a new default pager setting to the configuration, do the following:

1. Access the user EXEC mode by entering the **login** command or access the privileged EXEC mode by entering the **enable** command.

2. Enter the **pager** command.

If you use Telnet to access 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:

```
ciscoasa# terminal pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the “---More---” prompt. This command is saved to the configuration.
show running-config terminal	Displays the current terminal settings.
terminal	Allows syslog messages to display in 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.

Command Default

The default display width is 80 columns.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa# 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 ASA 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 ASA, 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*] [**ad-agent**] }

Syntax Description

ad-agent	Tests connectivity to the AAA AD agent server.
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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was added.
8.4(2)	The **ad-agent** keyword was added.

Usage Guidelines

The **test aaa-server** command lets you verify that the ASA 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 ASA.

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.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)#
authentication-port 1650
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(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:

```
ciscoasa# 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 aaa-server ad-agent

To test the Active Directory Agent configuration after you configure, use the **test aaa-server ad-agent** command in AAA Server Group configuration mode.

test aaa-server ad-agent

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa server group configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

To configure the Active Directory Agent for the Identity Firewall, you must enter the **ad-agent-mode** command, which is a submode of the **aaa-server** command. Entering the **ad-agent-mode** command enters the AAA Server Group configuration mode.

After configuring the Active Directory Agent, enter the **test aaa-server ad-agent** command to verify that the ASA has a functional connection to the Active Directory Agent.

Periodically or on-demand, the AD Agent monitors the Active Directory server security event log file via WMI for user login and logoff events. The AD Agent maintains a cache of user ID and IP address mappings. and notifies the ASA of changes.

Configure the primary and secondary AD Agents for the AD Agent Server Group. When the ASA detects that the primary AD Agent is not responding and a secondary agent is specified, the ASA switches to secondary AD Agent. The Active Directory server for the AD agent uses RADIUS as the communication protocol; therefore, you should specify a key attribute for the shared secret between ASA and AD Agent.

Examples

The following example shows how to enable **ad-agent-mode** while configuring the Active Directory Agent for the Identity Firewall and then test the connection:

```
hostname(config)# aaa-server adagent protocol radius
hostname(config)# ad-agent-mode
hostname(config-aaa-server-group)# aaa-server adagent (inside) host 192.168.1.101
hostname(config-aaa-server-host)# key mysecret
hostname(config-aaa-server-hostkey)# user-identity ad-agent aaa-server adagent
hostname(config-aaa-server-host)# test aaa-server ad-agent
```

Related Commands

Command	Description
aaa-server	Creates a AAA server group and configures AAA server parameters that are group-specific and common to all group hosts.
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

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

Command Default

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Normally the ASA 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 ASA 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.

```
ciscoasa
 #
test dynamic-access-policy attributes
ciscoasa
(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

To test already configured DAP records, use the test dynamic-access-policy execute command in privileged EXEC mode:

test dynamic-access-policy execute

Syntax Description

AAA attribute value	The DAP subsystem on the device references these values when evaluating the AAA and endpoint selection attributes for each record. • AAA Attribute—Identifies the AAA attribute. • Operation Value—Identifies the attribute as =/!= to the given value.
endpoint attribute value	Identifies the endpoint attribute. • Endpoint ID—Provides the endpoint attribute ID. • Name/Operation/Value—

Command Modes

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

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

Command History

Release	Modification
8.4(4)	This command was added.

Usage Guidelines

This command lets you test the retrieval of the set of DAP records configured on the device by specifying authorization attribute value pairs.

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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa# test
 regex farscape scape
INFO: Regular expression match succeeded.
ciscoasa# 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 (Deprecated)

Note The last supported release of this command was Version 9.5(1).

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.

Command Default

No default values or behavior.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

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 ASA acts as a proxy for the WebVPN user to the SSO server. The ASA 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:

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

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

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

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA 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 ASA 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.

Command Default

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config-webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

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

```
ciscoasa
(config)#
 webvpn
ciscoasa(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 blocksize

To configure the TFTP blocksize value, use **tftp blocksize** command in global configuration mode. To remove the blocksize configuration, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

tftp blocksize *number*
no tftp blocksize

Syntax Description

number	Specifies the blocksize value to be configured. This value can be between 513 and 8192 octets. A new default value is set for the blocksize—1456 octets.

Command Default

The new default value is 1456 octets. If the server does not supported this negotiation, the old default value—512 octets size prevail.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

The **tftp blocksize** command allows you to configure a larger blocksize to enhance the tftp file transfer speed. This configurable blocksize value option is appended to tftp read/write request and sent to tftp server for acknowledgement. On receiving the Option Acknowledgment (OACK), the file transfer is initiated with the configured blocksize value. The new default blocksize is 1456 octets. The **no** form of this command will reset the blocksize to the older default value—512 octets.

The **show running-configuration** command displays the configured blocksize value, except the default value.

Examples

The following example shows how to specify a TFTP blocksize value:

```
ciscoasa(config)# tftp blocksize 2048
ciscoasa(config)#
```

Related Commands

Command	Description
show running-config tftp blocksize	Displays the configured blocksize value, except the default value.

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

filename	Specifies the path and filename.
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.

Command Default

No default behavior or values.

Command Modes

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

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

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 ASA supports only one **tftp-server** command.

Examples

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

```
ciscoasa(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
ciscoasa(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.

tftp-server address (Deprecated)

To specify the TFTP servers in the cluster, use the **tftp-server address** command in phone-proxy configuration mode. To remove the TFTP server from the Phone Proxy configuration, use the **no** form of this command.

tftp-server address *ip_address* [*port*] **interface** *interface*
no tftp-server address *ip_address* [*port*] **interface** *interface*

Syntax Description

ip_address	Specifies the address of the TFTP server.
interface *interface*	Specifies the interface on which the TFTP server resides. This must be the real address of the TFTP server.
port	(Optional) This is the port the TFTP server is listening in on for the TFTP requests. This should be configured if it is not the default TFTP port 69.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

The Phone Proxy must have at least one CUCM TFTP server configured. Up to five TFTP servers can be configured for the Phone Proxy.

The TFTP server is assumed to be behind the firewall on the trusted network; therefore, the Phone Proxy intercepts the requests between the IP phones and TFTP server. The TFTP server must reside on the same interface as the CUCM.

Create the TFTP server using the internal IP address and specify the interface on which the TFTP server resides.

On the IP phones, the IP address of the TFTP server must be configured as follows:

- If NAT is configured for the TFTP server, use the TFTP server's global IP address.
- If NAT is not configured for the TFTP server, use the TFTP server's internal IP address.

If the service-policy is applied globally, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on all ingress interfaces, except for the interface on which the TFTP server resides. When the service-policy is applied on a specific interface, a classification rule will be created to direct any TFTP traffic reaching the TFTP server on that specified interface to the phone-proxy module.

If a NAT rule is configured for the TFTP server, it must be configured prior to applying the service-policy so that the global address of the TFTP server is used when installing the classification rule.

Examples

The following example shows the use of the **tftp-server address** command to configure two TFTP servers for the Phone Proxy:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.2 in interface outside
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.3 in interface outside
ciscoasa
(config-phone-proxy)#
media-termination address
192.168.1.4
 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address
192.168.1.25
 interface outside
ciscoasa
(config-phone-proxy)#
tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
ctl-file asactl
ciscoasa
(config-phone-proxy)#
cluster-mode nonsecure
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

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.

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

Table 1: Basic Threat Detection Default Settings

Packet Drop Reason	Trigger Settings	
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 20 second period.
	80 drops/sec over the last 3600 seconds.	320 drops/sec over the last 120 second period.
Scanning attack detected	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
	4 drops/sec over the last 3600 seconds.	8 drops/sec over the last 120 second period.
Incomplete session detected such as TCP SYN attack detected or UDP session with no return data attack detected (combined)	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 20 second period.
	80 drops/sec over the last 3600 seconds.	160 drops/sec over the last 120 second period.
Denial by access lists	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	640 drops/sec over the last 120 second period.
• Basic firewall checks failed • Packets failed application inspection	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 20 second period.
	320 drops/sec over the last 3600 seconds.	1280 drops/sec over the last 120 second period.

Packet Drop Reason	Trigger Settings	
Interface overload	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 20 second period.
	1600 drops/sec over the last 3600 seconds.	6400 drops/sec over the last 120 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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval was changed from 1/60th to 1/30th of the average rate.

Usage Guidelines

When you enable basic threat detection, the ASA 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 UDP session with no return data attack detected

When the ASA detects a threat, it immediately sends a system log message (733100) and alerts Adaptive Security Device Manager (ASDM).

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

Table 1.1 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 ASA sends a system message. The ASA 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 1/30th of the average rate interval or 10 seconds, whichever is higher. For each event received, the ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA 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:

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(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 1/30th 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 UDP session with no return data attack.

Command Default

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

Table 2: Basic Threat Detection Default Settings

Packet Drop Reason	Trigger Settings	
Average Rate	Burst Rate	
• **dos-drop**	100 drops/sec over the last 600 seconds.	400 drops/sec over the last 20 second period.
• **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	100 drops/sec over the last 3600 seconds.	400 drops/sec over the last 120 second period.
scanning-threat	5 drops/sec over the last 600 seconds.	10 drops/sec over the last 20 second period.
	5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 120 second period.
syn-attack	100 drops/sec over the last 600 seconds.	200 drops/sec over the last 20 second period.
	100 drops/sec over the last 3600 seconds.	200 drops/sec over the last 120 second period.
acl-drop	400 drops/sec over the last 600 seconds.	800 drops/sec over the last 20 second period.
	400 drops/sec over the last 3600 seconds.	800 drops/sec over the last 120 second period.
• **fw-drop** • **inspect-drop**	400 drops/sec over the last 600 seconds.	1600 drops/sec over the last 20 second period.
	400 drops/sec over the last 3600 seconds.	1600 drops/sec over the last 120 second period.
interface-drop	2000 drops/sec over the last 600 seconds.	8000 drops/sec over the last 20 second period.
	2000 drops/sec over the last 3600 seconds.	8000 drops/sec over the last 120 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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.

Usage Guidelines

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

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

When the ASA 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 1.1 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 ASA sends a system message. The ASA 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 ASA checks the average and burst rate limits; if both rates are exceeded, then the ASA 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:

```
ciscoasa(config)# threat-detection basic-threat
ciscoasa(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 ASA identifies the host as an attacker, in addition to sending syslog message 733101.

Command Default

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

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

Table 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 20 second period.
5 drops/sec over the last 3600 seconds.	10 drops/sec over the last 120 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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	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 ASA 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 ASA performance and memory significantly while it creates and gathers host- and subnet-based data structure and information.

You can configure the ASA to send system log messages about an attacker or you can automatically shun the host. By default, the system log message 730101 is generated when a host is identified as an attacker. Be sure to except addresses from shunning when you expect a lot of messages from the host. For example, if you have enabled PIM multicast, exempt the PIM routers or PIM messages will be dropped.

The ASA identifies attackers and targets when the scanning threat event rate is exceeded. The ASA 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 ASA 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.

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

Command	Description
show threat-detection scanning-threat	Shows the hosts that are categorized as attackers and targets.
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 service

To configure Threat Detection for VPN Services, use the **threat-detection service** command in global configuration mode

threat-detection service { **remote-access-authentication** | **remote-access-client-initiations** }
hold-down *minutes* **threshold** *count*
threat-detection service invalid-vpn-access
no threat-detection service *service_name*

Syntax Description

hold-down *minutes*	Defines the hold-down period from the last failure or initiation. The threshold count of consecutive failures/initiations must be met within the hold-down period of the previous failure/initiation to trigger a shun for the attacker's IPv4 address. For example, if the hold-down period is 10 minutes and the threshold is 20, and if there are 20 consecutive authentication failures from a single IPv4 address, and if the timespan between any two consecutive failures does not exceed 10 minutes, then the source IPv4 address will be shunned. You can specify a time between 1 and 1440 minutes.
invalid-vpn-access (*service_name*)	Protect against attempts to connect to an invalid VPN service, that is, services that are for internal use only. An IP address that attempts this connection is immediately shunned.
remote-access-authentication (*service_name*)	Protect against remote access VPN login authentication attacks. By repeatedly starting login attempts in a password-spray attack, the attacker can consume resources used for authentication attempts, thus preventing real users from logging into the VPN.
remote-access-client-initiations (*service_name*)	Protect against client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. Like the password-spray attack, this attack can consume resources and prevent valid users from connecting to the VPN.
threshold *count*	Defines the number of failed attempts that must occur within the hold-down period to trigger the shun. The allowed range for this parameter differs by service: • **remote-access-authentication**—You can specify a threshold between 1 and 100. • **remote-access-client-initiations**—You can specify a threshold between 5 and 100.

Command Default

All services are disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.16(4), 9.20(3)	This command was introduced.

Usage Guidelines

When you enable these services, the system automatically shuns hosts that exceed thresholds to prevent further attempts. You can manually remove the shun using the **no shun** command for the address.

When deciding on appropriate hold-down and threshold values, consider the use of NAT in your environment. If you use PAT, so that many requests can come from the same IP address, then you should consider higher values for the authentication failure and client initiation services, to ensure valid users have enough time to complete their connections. For example, a hotel, where many customers might try connecting within very short time periods.

Example

The following example enables the Remote Access Authentication service and sets a metric of 10 failures within 20 minutes.

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

The following example enables the Remote Access Client Initiations service and sets a metric of 10 initiations within 20 minutes.

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

The following example enables the Invalid VPN Access service. You cannot set hold-down and thresholds for this service, as any attempt is immediately shunned.

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

Related Commands

Command	Description
clear shun	Removes all shuns.
clear threat-detection service	Clears threat detection service entries and statistics.

Command	Description
show threat-detection service	Shows statistics and entries for Threat Detection for VPN Services.
[no]shun	Shuns an address, or clears the shun on a specific address.

threat-detection statistics

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

Caution Enabling statistics can affect the ASA 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 | port | protocol** [**number-of-rate** { **1 | 2 | 3** }] | **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 statistics 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, port, or protocol statistics. The default number of rate intervals is **1** , which keeps the memory usage low. To view more rate intervals, set the value to **2** or **3** . For example, if you set the value to **3** , then you view data for the last 1 hour, 8 hours, and 24 hours. If you set this keyword to **1** (the default), 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 ASA samples the number of attacks 30 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.

Command Default

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:

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

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)/8.1(2)	The **tcp-intercept** keyword was added.
8.1(2)	The **number-of-rates** keyword was added for host statistics, and the default number of rates was changed from 3 to 1.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.3(1)	The **number-of-rates** keyword was added for port and protocol statistics, and the default number of rates was changed from 3 to 1.

Usage Guidelines

If you do not specify any options in this command, then you enable all statistics. To enable only certain statistics, enter this command for each statistic type, and do not also enter the command without any options. You can enter **threat-detection statistics** (without any options) and then customize certain statistics by entering the command with statistics-specific options (for example, **threat-detection statistics host number-of-rate 2**). If you enter **threat-detection statistics** (without any options) and then enter a command for specific statistics, but without any statistic-specific options, then that command has no effect because it is already enabled.

If you enter the **no** form of this command, it removes all **threat-detection statistics** commands, including the **threat-detection statistics access-list** command, which is enabled by default.

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:

```
ciscoasa(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
ciscoasa(config)# threat-detection statistics access-list
ciscoasa(config)# threat-detection statistics port
ciscoasa(config)# threat-detection statistics protocol
ciscoasa(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 memory	Shows the memory use for advanced threat detection 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.

Command Default

The default threshold is 5000 milliseconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.

Command	Description
timeout	Defines the amount of time the SLA operation waits for a response.

throughput level

To set the throughput level for the smart licensing entitlement request, use the **throughput level** command in license smart configuration mode. To remove the throughput level and unlicense your device, use the **no** form of this command.

Note This feature is supported on the ASA virtual only.

throughput level { **100M | 1G | 2G** }
no throughput level [**100M | 1G | 2G**]

Syntax Description

100M	Sets the throughput level to 100 Mbps.
1G	Sets the throughput level to 1 Gbps.
2G	Sets the throughput level to 2 Gbps.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
License smart configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

When you request or change the throughput level, you must exit license smart configuration mode for your changes to take effect.

Examples

The following example sets the feature tier to standard, and the throughput level to 2G:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

ticket (Deprecated)

To configure the ticket epoch and password for the Cisco Intercompany Media Engine proxy, use the **ticket** command in UC-IME configuration mode. To remove the configuration from the proxy, use the **no** form of this command.

ticket epoch *n* **password** *password*
no ticket epoch *n* **password** *password*

Syntax Description

n	Specifies the length of time between password integrity checks. Enter an integer from 1-255.
password	Sets the password for the Cisco Intercompany Media Engine ticket. Enter a minimum of 10 and a maximum of 64 printable character from the US-ASCII character set. The allowed characters include 0x21 to 0x73 inclusive, and exclude the space character. Only one password can be configured at a time.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
UC-IME configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.
9.4(1)	This command was deprecated along with all **uc-ime** mode commands.

Usage Guidelines

Configures the ticket epoch and password for Cisco Intercompany Media Engine.

The epoch contains an integer that updates each time that the password is changed. When the proxy is configured the first time and a password entered for the first time, enter 1 for the epoch integer. Each time you change the password, increment the epoch to indicate the new password. You must increment the epoch value each time your change the password.

Typically, you increment the epoch sequentially; however, the ASA allows you to choose any value when you update the epoch.

If you change the epoch value, the current password is invalidated and you must enter a new password.

We recommend a password of at least 20 characters. Only one password can be configured at a time.

The ticket password is stored onto flash. The output of the **show running-config uc-ime** command displays ***** instead of the password string.

Note The epoch and password that you configure on the ASA must match the epoch and password configured on the Cisco Intercompany Media Engine server. See the Cisco Intercompany Media Engine server documentation for information.

Examples

The following example shows specify the ticket and epoch in the Cisco Intercompany Media Engine Proxy:

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
hostname(config-uc-ime)# fallback monitoring timer 120
hostname(config-uc-ime)# fallback hold-down timer 30
```

Related Commands

Command	Description
show running-config uc-ime	Shows the running configuration of the Cisco Intercompany Media Engine proxy.
uc-ime	Creates the Cisco Intercompany Media Engine proxy instance on the ASA.

timeout (aaa-server host)

To specify the length of time during which the ASA attempts to make a connection to a 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 (1-300 seconds) for the server. For each AAA transaction the ASA retries connection attempts (based on the interval defined on the **retry-interval** command) until the timeout is reached. If the number of consecutive failed transactions reaches the limit specified on the **max-failed-attempts** command in the AAA server group, the AAA server is deactivated and the ASA starts sending requests to another AAA server if it is configured.

Command Default

The default timeout value is 10 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid for all AAA server protocol types.

Use the **retry-interval** command to specify the amount of time the ASA waits between connection attempts. These intervals happen within the overall timeout, so if you have a long retry interval, the system will be able to make fewer retry attempts within the overall timeout. In practice, the retry interval should be less than the timeout interval.

Use the **max-failed-attempts** command to specify the maximum number of consecutive failed AAA transactions before deactivating a failed server. A AAA transaction is a sequence of an initial request and all retries. For the RADIUS protocol, the initial request and all the retries have same RADIUS packet identifier in the RADIUS protocol header.

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host 10.2.3.4 to use a timeout value of 30 seconds, with a retry interval of 10 seconds.

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
```

```
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 10.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 30
ciscoasa
(config-aaa-server-host)# retry-interval 10
ciscoasa
(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)

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 ASA retries the list of servers, this timeout doubles. Use the **retries** command in dns-server-group configuration mode to configure the number of retries.

Command Default

The default timeout is 2 seconds.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

Examples

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

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# 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 ASA does not receive a response.
show running-config dns server-group	Shows the current running DNS server-group configuration.

timeout (global)

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 **clear configure timeout** command. To reset a single feature to its default, reenter the **timeout** command with the default value.

timeout { **conn | conn-holddown | floating-conn | h225 | h323 | half-closed | icmp | icmp-error | igp stale-route | mgcp | mgcp-pat | pat-xlate | sctp | sip | sip-disconnect | sip-invite | sip_media | sip-provisional-media | sunrpc | tcp-proxy-reassembly | udp | xlate** } *hh:mm:ss*
timeout uauth *hh:mm:ss* [**absolute | inactivity**]

Syntax Description

absolute	(Optional for **uauth**) 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	Specifies the idle time after which a connection closes, between 0:5:0 and 1193:0:0. The default is 1 hour (1:0:0). Use 0 to never time out a connection.
conn-holddown	How long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. The purpose of the connection holddown timer is to reduce the effect of route flapping, where routes might come up and go down quickly. You can reduce the holddown timer to make route convergence happen more quickly. The default is 15 seconds, the range is 00:00:00 to 00:00:15.
floating-conn	When multiple routes exist to a network with different metrics, the ASA uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0.
hh:*mm*:*ss*	Specifies the timeout in hours, minutes, and seconds. Use 0 to never time out a connection, if available.
h225	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 0:0:1 disables the timer and closes the TCP connection immediately after all calls are cleared.
h323	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	Specifies the idle time after which a TCP half-closed connection will be freed, between 0:5:0 (for 9.1(1) and earlier) or 0:0:30 (for 9.1(2) and later) and 1193:0:0. The default is 10 minutes (0:10:0). Use 0 to never time out a connection. A connection is considered half-closed if both the FIN and FIN-ACK have been seen. If only the FIN has been seen, the regular **conn** timeout applies.

icmp	Specifies the idle time for ICMP, between 0:0:2 and 1193:0:0 The default is 2 seconds (0:0:2).
icmp-error	Specifies the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet, between 0:0:0 and 0:1:0 or the **timeout icmp** value, whichever is lower. The default is **0** (disabled). When this timeout is disabled, and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors.
igp stale-route	Specifies the idle time for how long to keep a stale route before removing it from the router information base. These routes are for interior gateway protocols such as OSPF. The default is 70 seconds (00:01:10), the range is 00:00:10 to 00:01:40.
inactivity	(Optional for **uauth**) Requires uauth reauthentication after the inactivity timeout expires.
mgcp	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	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).
pat-xlate	Specifies the idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.
sctp	Specifies the idle time until a Stream Control Transmission Protocol (SCTP) connection closes, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).
sip	Specifies the idle 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	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 00:10:0. 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	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 for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
sip-provisional-media	Specifies timeout value for SIP provisional media connections, between 0:1:0 and 1193:0:0. The default is 2 minutes (0:2:0).

sunrpc	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	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	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	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	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).

Command Default

The defaults are as follows:

conn is 1 hour (**1:0:0**).

- **conn-holddown** is 15 seconds (**0:0:15**)
- **floating-conn** never times out (**0**)
- **h225** is 1 hour (**1:0:0**).
- **h323** is 5 minutes (**0:5:0**).
- **half-closed** is 10 minutes (**0:10:0**).
- **icmp** is 2 seconds (**0:0:2**)
- **icmp-error** never times out (**0**)
- **igp stale-route** is 70 seconds (**00:01:10**)
- **mgcp** is 5 minutes (**0:5:0**).
- **mgcp-pat** is 5 minutes (**0:5:0**).
- **rpc** is 5 minutes (**0:5:0**).
- **sctp** is 2 minutes (**0:2:0**).
- **sip** is 30 minutes (**0:30:0**).
- **sip-disconnect** is 2 minutes (**0:2:0**).
- **sip-invite** s 3 minutes (**0:3:0**).
- **sip_media** is 2 minutes (**0:2:0**).
- **sip-provisional-media** is 2 minutes (**0:2:0**).
- **sunrpc** is 10 minutes (**0:10:0**)

- **tcp-proxy-reassembly** is 1 minute (**0:1:0**)
- **uauth** is 5 minutes (**0:5:0**) **absolute**.
- **udp** is 2 minutes (**0:02:0**).
- **xlate** is 3 hours (**3:0:0**).

Command Modes

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

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

Command History

Release	Modification
7.2(1)	The **mgcp-pat,** sip-disconnect, and sip-invite keywords were added.
7.2(4)/8.0(4)	The **sip-provisional-media** keyword was added.
7.2(5)/8.0(5)/8.1(2)/8.2(1)	The **tcp-proxy-reassembly** keyword was added.
8.2(5)/8.4(2)	The **floating-conn** keyword was added.
8.4(3)	The **pat-xlate** keyword was added.
9.1(2)	The minimum **half-closed** value was lowered to 30 seconds (0:0:30).
9.4(3)/9.6(2)	The **conn-holddown** keyword was added.
9.5(2)	The **sctp** keyword was added.
9.7(1)	The **igp stale-route** keyword was added.
9.8(1)	The **icmp-error** 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:

```
ciscoasa(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
ciscoasa(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 (policy-map type inspect gtp > parameters)

To change the inactivity timers for a GTP session, use the **timeout** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect gtp** command. Use the **no** form of this command to set these intervals to their default values.

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

Syntax Description

hh:*mm*:*ss*	The idle timeout for the specified service (in hour:minute:second format). To have no timeout, specify 0 for the number.
endpoint	The maximum period of inactivity before a GTP endpoint is removed.
gsn	The maximum period of inactivity before a GSN is removed. Starting in 9.5(1), this keyword is removed and replaced by the **endpoint** keyword.
pdp-context	The maximum period of inactivity before removing the PDP context for a GTP session. In GTPv2, this is the bearer context.
request	The maximum period of inactivity after which a request is removed from the request queue. Any subsequent responses to a dropped request will also be dropped.
signaling	The maximum period of inactivity before GTP signaling is removed.
t3-response	The maximum wait time for a response before removing the connection.
tunnel	The maximum period of inactivity for the GTP tunnel before it is torn down.

Command Default

The default is 30 minutes for **endpoint**, **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).

The default for **t3-response** is 20 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Release	Modification
9.5(1)	The **gsn** keyword was replaced by **endpoint**.

Usage Guidelines

Use this command to change the default timeouts used in GTP inspection.

Examples

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

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout request 00:02:00
```

Related Commands

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

timeout (policy-map type inspect m3ua > parameters)

To change the inactivity timers for an M3UA session, use the **timeout** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect m3ua** command. Use the **no** form of this command to set these intervals to their default values.

timeout { **endpoint | session** } *hh:mm:ss*
no timeout { **endpoint | session** } *hh:mm:ss*

Syntax Description

hh:mm:ss	The idle timeout for the specified service (in hour:minute:second format). To have no timeout, specify 0 for the number.
endpoint	The maximum period of inactivity before statistics for an M3UA endpoint are removed. The default is 30 minutes.
session	The idle timeout to remove an M3UA session if you enable strict ASP state validation, in hh:mm:ss format. The default is 30 minutes (00:30:00). Disabling this timeout can prevent the system from removing stale sessions.

Command Default

The default is 30 minutes for **endpoint** and **session**.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	This command was added.
9.7(1)	The **session** keyword was added.

Usage Guidelines

Use this command to change the default timeouts used in M3UA inspection.

Examples

The following example sets a 45 minute timeout for endpoints.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.
show service-policy inspect m3ua	Displays M3UA statistics.
strict-asp-state	Enables strict M3UA ASP state validation.

timeout (policy-map type inspect radius-accounting > parameters)

To change the inactivity timers for RADIUS accounting users, use the **timeout** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type 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.

Command Default

The default timeout for users is one hour.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Examples

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

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(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 (type echo)

To set the amount of time the SLA operation waits for a response to the request packets, use the **timeout** command in type echo configuration mode. You can access the type echo configuration mode by first entering the **sla monitor** command.To restore the default value, use the **no** form of this command.

timeout *milliseconds*
no timeout

Syntax Description

milliseconds	0 to 604800000.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Type echo configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

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.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(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 assertion

To configure the SAML timeout, use the **timeout assertion** command in webvpn configuration mode:

timeout assertion *number of seconds*

Syntax Description

number of seconds	SAML IdP timeout, in seconds, from 1 - 7200.

Command Default

The default is none, which means that NotBefore and NotOnOrAfter in the assertion determines the validity.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config webVPN	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5.2	This command was added.

Usage Guidelines

If specified, this configuration overrides NotOnOrAfter if the sum of NotBefore and timeout-in-seconds is earlier than NotOnOrAfter. If not specified, NotBefore and NotOnOrAfter in the assertion is used to determine the validity. When you input a timeout value under config-webvpn-saml-idp, both assertion and the number of seconds value are mandatory.

Examples

The following example configures the clientless VPN base URL, SAML request signature, and SAML assertion timeout:

```
ciscoasa(config-webvpn-saml-idp)# base url https://172.23.34.222
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 7200
```

timeout edns

To configure the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server, use the **timeout edns** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

timeout edns *hh:mm:ss*
no timeout edns *hh:mm:ss*

Syntax Description

hh:mm:ss	The idle timeout for a connection from the client to the Umbrella server (in hour:minute:second format), from 0:0:0 to 1193:0:0. The default is 0:02:00 (2 minutes). To have no timeout, specify 0 for the number.

Command Default

The default is 0:02:00 (2 minutes).

Command Modes

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

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

Command History

Release	Modification
9.10(1)	This command was added.

Examples

The following example sets a one minute idle timeout for connections from a client to the Umbrella server.

```
ciscoasa(config)# umbrella-global

ciscoasa(config)# timeout edns 0:1:0
```

Related Commands

Commands	Description
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
umbrella-global	Configures the Cisco Umbrella global parameters.

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.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Examples

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

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(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.

timeout secure-phones (Deprecated)

To configure the idle timeout after which the secure-phone entry is removed from the Phone Proxy database, use the **timeout secure-phones** command in phone-proxy configuration mode. To set the timeout value back to the default of 5 minutes, use the **no** form of this command.

timeout secure-phones *hh:mm:ss*
no timeout secure-phones *hh:mm:ss*

Syntax Description

hh:mm:ss	Specifies the idle timeout after which the object is removed. The default is 5 minutes.

Command Default

The default value for secure phone timeout is 5 minutes.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

Since secure phones always request a CTL file upon bootup, the Phone Proxy creates a database that marks the phone as secure. The entries in the secure phone database are removed after a specified configured timeout (via the **timeout secure-phones** command). The entry's timestamp is updated for each registration refresh the Phone Proxy receives for SIP phones and KeepAlives for SCCP phones.

The default value for the **timeout secure-phones** command is 5 minutes. Specify a value that is greater than the maximum timeout value for SCCP KeepAlives and SIP Register refresh. For example, if the SCCP Keepalives are configured for 1 minute intervals and the SIP Register Refresh is configured for 3 minutes, configure this timeout value greater than 3 minutes.

Examples

The following example shows the use of the **timeout secure-phones** command to configure the Phone Proxy to timeout entries in the secure phone database after 3 minutes:

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa
(config-phone-proxy)#
tftp-server address 192.168.1.2 in interface outside
ciscoasa
(config-phone-proxy)#
```

```
tftp-server address 192.168.1.3 in interface outside
ciscoasa
(config-phone-proxy)#
media-termination address 192.168.1.4
ciscoasa
(config-phone-proxy)#
tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
ctl-file asactl
ciscoasa(config-phone-proxy)# timeout secure-phones 00:03:00
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 ASA; 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:

```
ciscoasa(config)# time-range New_York_Minute
ciscoasa(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”:

```
ciscoasa(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
ciscoasa(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 ASA.
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 nsf wait

To adjust nsf wait timer, use the timers nsf wait command in router ospf configuration mode. To reset the OSPF timing defaults, use the no form of this command.

timers nsf wait *interval*
no timers nsf wait *interval*

Syntax Description

interval	Interface wait interval (in seconds) during NSF restart. The default is 20 seconds. The range is from 0 to 65535.

Command Default

The default value of nsf wait timer is 20 seconds.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

OSPF routers are expected to set the RS-bit in the EO-TLV attached to a Hello packet when it is not known that all neighbors are listed in the packet, but the restarting router require to preserve their adjacencies. However, the RS-bit value must not be longer than the RouterDeadInterval seconds. Use the **timer nsf wait** command to set the the RS-bit in Hello packets lesser than RouterDeadInterval seconds.

Examples

The following example shows configuration of the nsf wait interval in seconds:

```
ciscoasa(config)# router ospf 1
ciscoasa(config-router)# timers ?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
router mode commands/options:
  wait  Interface wait interval during NSF restart
ciscoasa(config-router)# timers nsf wait ?
router mode commands/options:
  <1-65535>  Seconds
ciscoasa(config-router)# timers nsf wait 35
ciscoasa(config-router)#
```

timers bgp

To adjust BGP network timers, use the timers bgp command in router bgp configuration mode. To reset the BGP timing defaults, use the no form of this command.

timers bgp *keepalive holdtime* [*min-holdtime*]
no timers bgp *keepalive holdtime* [*min-holdtime*]

Syntax Description

keepalive	Frequency (in seconds) with which the Cisco IOS software sends keepalive messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
holdtime	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
min-holdtime	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the holdtime argument. The range is from 0 to 65535.

Command Default

keepalive: 60 secondsholdtime: 180 seconds

Command Modes

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

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

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

When configuring the holdtime argument for a value of less than twenty seconds, the following warning is displayed: A hold time of less than 20 seconds increases the chances of peer flapping

If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed: Minimum acceptable hold time should be less than or equal to the configured hold time

Note When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating “unacceptable hold time.”

Examples

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# timers bgp 70 130 100
```

timers lsa arrival

To set the minimum interval at which the ASA accepts the same LSA from OSPFv3 neighbors, use the **timers lsa arrival** command in IPv6 router configuration mode. To restore the default value, use the **no** form of this command.

timers lsa arrival *milliseconds*
no timers lsa arrival *milliseconds*

Syntax Description

milliseconds	Specifies the minimum delay in milliseconds that must pass between acceptance of the same LSA that is arriving between neighbors. Valid values are from 0 to 600,000 milliseconds.

Command Default

The default is 1000 milliseconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to indicate the minimum interval that must pass between acceptance of the same LSA that is arriving from neighbors.

Examples

The following example sets the minimum interval for accepting the same LSA at 2000 milliseconds:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# log-adjacency-changes
ciscoasa(config-rtr)# timers lsa arrival 2000
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.

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.

Command Default

The default interval is 240 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config-rtr)# timers lsa-group-pacing 500
ciscoasa(config-rtr)#
```

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 pacing flood

To configure LSA flood packet pacing, use the **timers pacing flood** command in IPv6 router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*
no timers pacing flood *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds at which LSAs in the flooding queue are paced in-between updates. The configurable range is from 5 to 100 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure LSA flood packet pacing.

Examples

The following example configures LSA flood packet pacing updates to occur in 20-millisecond intervals for OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
timers pacing lsa-group	Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

timers pacing flood

To configure LSA flood packet pacing, use the **timers pacing flood** command in IPv6 router configuration mode. To restore the default flood packet pacing value, use the **no** form of this command.

timers pacing flood *milliseconds*
no timers pacing flood *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds at which LSAs in the flooding queue are paced in-between updates. The configurable range is from 5 to 100 milliseconds.

Command Default

The default is 33 milliseconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure LSA flood packet pacing.

Examples

The following example configures LSA flood packet pacing updates to occur in 20-millisecond intervals for OSPFv3:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing flood 20
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
timers pacing lsa-group	Specifies the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

timers pacing lsa-group

To specify the interval at which OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged, use the **timers pacing lsa-group** command in IPv6 router configuration mode. To restore the default value, use the **no** form of this command.

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

Syntax Description

seconds	Specifies the number of seconds in the interval at which LSAs are collected into a group and refreshed, check summed, or aged. Valid values are from 10 to 1800 seconds.

Command Default

The default interval is 240 seconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to indicate the interval at which the OSPFv3 LSAs are collected into a group and refreshed, check summed, or aged.

Examples

The following example configures OSPFv3 group packet pacing updates between LSA groups to occur in 300-seconds intervals for OSPFv3 routing process 1:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.
timers pacing retransmission	Configures LSA retransmission packet pacing.

timers pacing retransmission

To configure link-state advertisement (LSA) retransmission packet pacing, use the timers pacing retransmission command in router configuration mode. To restore the default retransmission packet pacing value, use the no form of this command.

timers pacing retransmission *milliseconds*
no timers pacing retransmission

Syntax Description

milliseconds	Specifies the time interval in milliseconds at which LSAs in the retransmission queue are paced. Valid values are from 5 milliseconds to 200 milliseconds.

Command Default

The default interval is 66 milliseconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Configuring Open Shortest Path First (OSPF) retransmission pacing timers allow you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue. This command allows you to control the rate at which LSA updates occur so that high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs can be reduced. The default settings for OSPF packet retransmission pacing timers are suitable for the majority of OSPF deployments.

Note Do not change the packet retransmission pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default flooding timers.

Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default packet retransmission pacing timer values.

Examples

The following example configures LSA flood pacing updates to occur in 55-millisecond intervals for OSPF routing process 1:

```
hostname(config)# router ospf 1
hostname(config-router)# timers pacing retransmission 55
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers pacing flood	Configures LSA flood packet pacing for OSPFv3 routing processes.

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.

Command Default

The defaults are as follows:

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

```
ciscoasa(config-router)# timers spf 10 20
ciscoasa(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.

timers throttle

To set rate-limiting values for Open Shortest Path First (OSPF) link-state advertisement (LSA) generation or SPF generation, use the timers throttle command in router ospf or ipv6 router ospf configuration mode. To restore the default values, use the no form of this command.

timers throttle { **lsa | spf** } *start-interval hold-interval max-interval*
no timers throttle { **lsa | spf** }

Syntax Description

lsa	Configures LSA throttling.
start-interval	Specifies the delay in milliseconds to generate the first occurrence of the LSA. Specifies the delay in milliseconds to receive a change to the SPF calculation. Specifies the minimum delay in milliseconds to generate the first occurrence of LSAs. **Note** The first instance of LSA is generated immediately after a local OSPF topology change. The next LSA is generated only after start-interval. Valid values are between 0 and 0 to 600,000 milliseconds. The default value is 0 milliseconds; the LSA is sent immediately.
hold-interval	Specifies the maximum delay in milliseconds to originate the same LSA. Specifies the delay in milliseconds between the first and second SPF calculations. Specifies the minimum delay in milliseconds to generate the LSA again.This value is used to calculate the subsequent rate limiting times for LSA generation. Valid values are between 1 and 600,000 milliseconds. The default value is 5000 milliseconds.
max-interval	Specifies the minimum delay in milliseconds to originate the same LSA. Specifies the maximum wait time in milliseconds for SPF calculations. Specifies the maximum delay in milliseconds to generate the LSA again. Valid values are between 1 and 600,000 milliseconds. The default value is 5000 milliseconds.
spf	Configures SPF throttling.

Command Default

LSA throttling:

- For *start-interval* , the default value is 0 milliseconds.
- For *hold-interval* , the default value is 5000 milliseconds.
- For *max-interval* , the default value is 5000 milliseconds.

SPF throttling:

- For *start-interval* , the default value is 5000 milliseconds.
- For *hold-interval* , the default value is 10000 milliseconds.
- For *max-interval* , the default value is 10000 milliseconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	• Yes	—
Router ospf configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.2(1)	Added support for IPv6.

Usage Guidelines

LSA and SPF throttling provide a dynamic mechanism to slow down LSA updates in OSPF during times of network instability and allow faster OSPF convergence by providing LSA rate limiting in milliseconds.

For LSA throttling, if the minimum or maximum time is less than the first occurrence value, then OSPF automatically corrects to the first occurrence value. Similarly, if the maximum delay specified is less than the minimum delay, then OSPF automatically corrects to the minimum delay value.

For SPF throttling, if *hold-interval* or *max-interval* is less than *start-interval* , then OSPF automatically corrects to the *start-interval* value. Similarly, if *max-interval* is less than *hold-interval* , then OSPF automatically corrects to the *hold-interval* value.

Examples

The following example configures OSPFv3 LSA throttling in milliseconds:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle lsa 100 4000 5000
```

For LSA throttling, the following example shows the automatic correction that occurs if the maximum delay value specified is less than the minimum delay value:

```
ciscoasa(config)# ipv6 router ospf 10

ciscoasa(config-rtr)# timers throttle lsa 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6

ipv6 router ospf 10
 timers throttle lsa 100 100 100
```

The following example configures OSPFv3 SPF throttling in milliseconds:

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

For SPF throttling, the following example shows the automatic correction that occurs if the maximum delay value specified is less than the minimum delay value:

```
ciscoasa(config)# ipv6 router ospf 10

ciscoasa(config-rtr)# timers throttle spf 100 50 50
% OSPFv3: Throttle timers corrected to: 100 100 100
ciscoasa(config-rtr)# show running-config ipv6

ipv6 router ospf 10
 timers throttle spf 100 100 100
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
timers lsa-group-pacing	Specifies the interval at which OSPFv3 LSAs are collected and refreshed, checksummed, or aged.

timestamp

To define an action when the Time Stamp (TS) option occurs in a packet header with IP Options inspection, use the **timestamp** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

timestamp action { **allow | clear** }
no timestamp action { **allow | clear** }

Syntax Description

allow	Allow packets containing the Time Stamp IP option.
clear	Remove the Time Stamp option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Time Stamp IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

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

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# timestamp action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
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.

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).

Command Default

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:

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

Command History

Release	Modification
7.1(1)	This command was added.

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”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(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.