CHAPTER 24

same-security-traffic through show asdm sessions Commands

same-security-traffic

To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the **same-security-traffic** command in global configuration mode. To disable the same-security traffic, use the **no** form of this command.

same-security-traffic permit {**inter-interface | intra-interface**}

no same-security-traffic permit {**inter-interface | intra-interface**}

Syntax Description

inter-interface	Permits communication between different interfaces that have the same security level.
intra-interface	Permits communication in and out of the same interface.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **intra-interface** keyword now allows all traffic to enter and exit the same interface, and not just IPSec traffic.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) provides the following benefits:

- You can configure more than 101 communicating interfaces. If you use different levels for each interface, you can configure only one interface per level (0 to 100).
- You can allow traffic to flow freely between all same security interfaces without access lists.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed. This feature might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the security appliance is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the security appliance and then out again to the other spoke.

Note All traffic allowed by the **same-security-traffic intra-interface** command is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the security appliance.

Examples

The following example shows how to enable the same-security interface communication:

```
hostname(config)# same-security-traffic permit inter-interface
```

The following example shows how to enable traffic to enter and exit the same interface:

```
hostname(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
show running-config same-security-traffic	Displays the **same-security-traffic** configuration.

sasl-mechanism

To specify a SASL (Simple Authentication and Security Layer) mechanism for authenticating an LDAP client to an LDAP server, use the **sasl-mechanism** command in aaa-server host configuration mode. The SASL authentication mechanism options are **digest-md5** and **kerberos**.

To disable an authentication mechanism, use the **no** form of this command.

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

Note Because the security appliance serves as a client proxy to the LDAP server for VPN users, the LDAP client referred to here is the security appliance.

Syntax Description

digest-md5	The security appliance responds with an MD5 value computed from the username and password.
kerberos	The security appliance responds by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.
server-group-name	Specifies the Kerberos aaa-server group, up to 64 characters.

Defaults

No default behavior or values. The security appliance passes the authentication parameters to the LDAP server in plain text.

Note We recommend that you secure LDAP communications with SSL using the **ldap-over-ssl** command if you have not configured SASL.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use this command to specify security appliance authentication to an LDAP server using SASL mechanisms.

Both the security appliance and the LDAP server can support multiple SASL authentication mechanisms. When negotiating SASL authentication, the security appliance retrieves the list of SASL mechanisms configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the security appliance and the server. The Kerberos mechanism is stronger than the Digest-MD5 mechanism. To illustrate, if both the LDAP server and the security appliance support both mechanisms, the security appliance selects Kerberos, the stronger of the mechanisms.

When disabling the SASL mechanisms, you must enter a separate **no** command for each mechanism you want to disable because they are configured independently. Mechanisms that you do not specifically disable remain in effect. For example, you must enter both of the following commands to disable both SASL mechanisms:

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

Examples

The following examples, entered in aaa-server host configuration mode, enable the SASL mechanisms for authentication to an LDAP server named ldapsvr1 with an IP address of 10.10.0.1. This example enables the SASL digest-md5 authentication mechanism:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
```

The following example enables the SASL Kerberos authentication mechanism and specifies kerb-servr1 as the Kerberos AAA server:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

sast

To specify the number of SAST certificates to create in the CTL record, use the **sast** command in ctl-file configuration mode. To set the number of SAST certificates in the CTL file back to the default value of 2, use the **no** form of this command.

sast *number_sasts*

no sast *number_sasts*

Syntax Description

number_sasts	Specifies the number of SAST keys to create. The default is 2. maximum allowed is 5.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
CTL-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

CTL files are signed by a System Administrator Security Token (SAST).

Because the Phone Proxy generates the CTL file, it needs to create the SAST key to sign the CTL file itself. This key can be generated on the security appliance. A SAST is created as a self-signed certificate.

Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.

Examples

The following example shows the use of the **sast** command to create 5 SAST certificates in the CTL file:

```
hostname(config-ctl-file)# sast 5
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

secondary

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

secondary

no secondary

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

secondary-color

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

secondary-color [*color*]

no secondary-color

Syntax Description

color	(Optional) Specifies the color. 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. • Name length maximum is 32 characters

Defaults

The default secondary color is HTML #CCCCFF, a lavender shade.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The number of RGB values recommended for use is 216, many fewer than the mathematical possibilities. Many displays can handle only 256 colors, and 40 of those look differently on MACs and PCs. For best results, check published RGB tables. To find RGB tables online, enter RGB in a search engine.

Examples

The following example shows how to set an HTML color value of #5F9EAO, which is a teal shade:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

Related Commands

Command	Description
title-color	Sets a color for the WebVPN title bar on the login, home page, and file access page

secondary-text-color

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

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

no secondary-text-color

Syntax Description

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

Defaults

The default secondary text color is black.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set the secondary text color to white:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

Related Commands

Command	Description
text-color	Sets a color for text in the WebVPN title bar on the login, home page and file access page

secure-unit-authentication

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

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel. With this feature enabled, the hardware client does not have a saved username and password.

Note With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

secure-unit-authentication {**enable** | **disable**}

no secure-unit-authentication

Syntax Description

disable	Disables secure unit authentication.
enable	Enables secure unit authentication.

Defaults

Secure unit authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware client(s) use.

If you require secure unit authentication on the primary security appliance, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable secure unit authentication for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
user-authentication	Requires users behind a hardware client to identify themselves to the security appliance before connecting.

security-level

To set the security level of an interface, use the **security-level** command in interface configuration mode. To set the security level to the default, use the **no** form of this command. The security level protects higher security networks from lower security networks by imposing additional protection between the two.

security-level *number*

no security-level

Syntax Description

number	An integer between 0 (lowest) and 100 (highest).

Defaults

By default, the security level is 0.

If you name an interface "inside" and you do not set the security level explicitly, then the security appliance sets the security level to 100 (see the **nameif** command). You can change this level if desired.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **nameif** command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

  For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  For same security interfaces, you can filter traffic in either direction.
- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

  Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.
- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

  For same security interfaces, you can configure **established** commands for both directions.

Normally, interfaces on the same security level cannot communicate. If you want interfaces on the same security level to communicate, see the **same-security-traffic** command. You might want to assign two interfaces to the same level and allow them to communicate if you want to create more than 101 communicating interfaces, or you want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

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

Examples

The following example configures the security levels for two interfaces to be 100 and 0:

```
hostname(config)# interface gigabitethernet0/0
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear local-host	Resets all connections.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
vlan	Assigns a VLAN ID to a subinterface.

send response

To send a RADIUS Accounting-Response Start and Accounting-Response Stop message to the sender of the RADIUS Accounting-Request Start and Stop messages, use the **send response** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

send response

no send response

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to send a response with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

Related Commands

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

seq-past-window

To set the action for packets that have past-window sequence numbers (the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window), use the **seq-past-window** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

seq-past-window {**allow** | **drop**}

no seq-past-window

Syntax Description

allow	Allows packets that have past-window sequence numbers. This action is only allowed if the **queue-limit** command is set to 0 (disabled).
drop	Drops packets that have past-window sequence numbers.

Defaults

The default action is to drop packets that have past-window sequence numbers.

Command Modes

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

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

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **seq-past-window**—In tcp-map configuration mode, you can enter the **seq-past-window** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the security appliance to allow packets that have past-window sequence numbers:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# seq-past-window allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
queue-limit	Sets the out-of-order packet limit.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

serial-number

To include the security appliance serial number in the certificate during enrollment, use the **serial-number** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

serial-number

no serial-number

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to not include the serial number.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

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

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

server

To specify a default e-mail proxy server, use the **server** command in the applicable e-mail proxy mode. To remove the attribute from the configuration, use the **no** version of this command. The security appliance sends requests to the default e-mail server when the user connects to the e-mail proxy without specifying a server. If you do not configure a default server, and a user does not specify a server, the security appliance returns an error.

server {*ipaddr or hostname*}

no server

Syntax Description

hostname	The DNS name of the default e-mail proxy server.
ipaddr	The IP address of the default e-mail proxy server.

Defaults

There is no default e-mail proxy server by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to set a default POP3S e-mail server with an IP address. of 10.1.1.7:

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server (tls-proxy)

To specify the proxy trustpoint certificate presented during TLS handshake, use the **server** command in TLS proxy configuration mode. To remove the configuration, use the **no** form of this command.

server trust-point *p_tp*

no server trust-point *p_tp*

Syntax Description

trust-point *p_tp*	Specifies the defined trustpoint.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **server** command in TLS proxy configuration mode to control the TLS handshake parameters for the security appliance as the TLS server role in TLS proxy. It specifies the proxy trustpoint certificate presented during TLS handshake. This value corresponds to the trustpoint defined by the **crypto ca trustpoint** command. It can be self-signed or enrolled with a certificate authority.

The **server** command takes precedence over the global **ssl trust-point** command.

Examples

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

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

Related Commands

Commands	Description
client	Sets the TLS handshake parameters for the security appliance as the TLS client role in TLS proxy.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

server authenticate-client

To enable the security appliance to authenticate the TLS client during TLS handshake, use the **server authenticate-client** command in tls-proxy configuration mode.

To bypass client authenticaion, use the **no** form of this command.

server authenticate-client

no server authenticate-client

Syntax Description

There are no keywords or arguments for this command.

Defaults

This command is enabled by default, which means the TLS client is required to present a certificate during handshake with the security appliance.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Use the **server authenticate-client** command to control whether a client authentication is required during TLS Proxy handshake. When enabled (by default), the security appliance sends a Certificate Request TLS handshake message to the TLS client, and the TLS client is required to present its certificate.

Use the **no** form of this command to disable client authentication. Disabling TLS client authentication is suitable when the security appliance must interoperate with CUMA client or clients such as a Web browser that are incapable of sending a client certificate.

Examples

The following example configures a TLS proxy instance with client authentication disabled:

```
hostname(config)# tls-proxy mmp_tls
hostname(config-tlsp)# no server authenticate-client
hostname(config-tlsp)# server trust-point cuma_server_proxy
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.

server-port

To configure a AAA server port for a host, use the **server-port** command in aaa-server host mode. To remove the designated server port, use the **no** form of this command:

server-port *port-number*

no server-port

Syntax Description

port-number	A port number in the range 0 through 65535.

Defaults

The default server ports are as follows:

- SDI—5500
- LDAP—389
- Kerberos—88
- NT—139
- TACACS+—49

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example configures an SDI AAA server named “srvgrp1” to use server port number 8888:

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
```

Related Commands

Command	Description
aaa-server host	Configures host-specific AAA server parameters.

clear configure aaa-server	Removes all AAA-server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

server-separator

To specify a character as a delimiter between the e-mail and VPN server names, use **server-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the no form of this command.

server-separator {*symbol*}

no server-separator

Syntax Description

symbol	The character that separates the e-mail and VPN server names. Choices are "@," (at) "I" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Defaults

The default is "@" (at).

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The server separator must be different from the name separator.

Examples

The following example shows how to set a pipe (|) as the server separator for IMAP4S:

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

Related Commands

Command	Description
name-separator	Separates the e-mail and VPN usernames and passwords.

server-type

To manually configure the LDAP server model, use the **server-type** command in aaa-server host configuration mode. The security appliance supports the following server models:

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server, formerly named the Sun ONE Directory Server
- Generic LDAP directory servers that comply with LDAPv3 (no password management)

To disable this command, use the **no** form of this command.

server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

no server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

Syntax Description

auto-detect	Specifies that the security appliance determines the LDAP server type through auto-detection.
generic	Specifies LDAP v3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers.
microsoft	Specifies that the LDAP server is a Microsoft Active Directory.
openldap	Specifies that the LDAP server is an OpenLDAP server.
novell	Specifies that the LDAP server is a Novell server.
sun	Specifies that the LDAP server is a Sun Microsystems JAVA System Directory Server.

Defaults

By default, auto-detection attempts to determine the server type.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.
8.0(2)	Support for the OpenLDAP and Novell server types was added.

Usage Guidelines

The security appliance supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server, the Microsoft Active Directory, and other LDAPv3 directory servers.

Note

- Sun—The DN configured on the security appliance to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—Password management features are not supported.

By default, the security appliance auto-detects whether it is connected to a Microsoft directory server, a Sun LDAP directory server, or a generic LDAPv3 server. However, if auto-detection fails to determine the LDAP server type and if you know the server is either a Microsoft or Sun server, you can use the **server-type** command to manually configure the server as either a Microsoft or a Sun Microsystems LDAP server.

Examples

The following example, entered in aaa-server host configuration mode, configures the server type for the LDAP server ldapsvr1 at IP address 10.10.0.1. The first example configures a Sun Microsystems LDAP server.

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
```

The following example specifies that the security appliance use auto-detection to determine the server type:

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
```

RelatedCommands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
sasl-mechanism	Configures SASL authentication between the LDAP client and server.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

server trust-point

To specify the proxy trustpoint certificate to present during TLS handshake, use the **server trust-point** command in TLS server configuration mode.

server trust-point *proxy_trustpoint*

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The trustpoint can be self-signed, enrolled with a certificate authority, or from an imported credential. The **server trust-point** command has precedence over the global **ssl trust-point** command.

The **server trust-point** command specifies the proxy trustpoint certificate presented during TLS handshake. The certificate must be owned by the security appliance (identity certificate). The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential.

Create TLS proxy instances for each entity that can initiate a connection. The entity that initiates the TLS connection is in the role of TLS client. Because the TLS Proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Note When you are creating the TLS proxy instance to use with the Phone Proxy, the server trustpoint is the internal Phone Proxy trustpoint created the CTL file instance. The trustpoint name is in the form *internal_PP_<ctl-file_instance_name>*

Examples

The following example shows the use of the **server trust-point** command to specify the proxy trustpoint certificate to present during TLS handshake:

```
hostname(config-tlsp)# server trust-point ent_y_proxy
```

Related Commands

Command	Description
client (tls-proxy)	Configures trustpoints, keypairs, and cipher suites for a TLS proxy instance.
client trust-point	Specifies the proxy trustpoint certificate to present during TLS handshake.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.
tls-proxy	Configures a TLS proxy instance.

service

To enable resets for denied TCP connections, use the **service** command in global configuration mode. To disable resets, use the **no** form of this command.

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

Syntax Description

interface *interface_name*	Enables or disables resets for the specified interface.
resetinbound	Sends TCP resets for all inbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. The security appliance also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets. If you do not specify an interface, then this setting applies to all interfaces.
resetoutbound	Sends TCP resets for all outbound TCP sessions that attempt to transit the security appliance and are denied by the security appliance based on access lists or AAA settings. The security appliance also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the security appliance silently discards denied packets. This option is enabled by default. You might want to disable outbound resets to reduce the CPU load during traffic storms, for example.
resetoutside	Enables resets for TCP packets that terminate at the least secure interface and are denied by the security appliance based on access lists or AAA settings. The security appliance also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. When this option is not enabled, the security appliance silently discards the packets of denied packets. We recommend that you use the **resetoutside** keyword with interface PAT. This keyword allows the security appliance to terminate the IDENT from an external SMTP or FTP server. Actively resetting these connections avoids the 30-second timeout delay.

Defaults

By default, **service resetoutbound** is enabled for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	The **interface** keyword and the **resetoutbound** command were added.

Usage Guidelines

You might want to explicitly send resets for inbound traffic if you need to reset identity request (IDENT) connections. When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance.

Examples

The following example disables outbound resets for all interfaces except for the inside interface:

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

The following example enables inbound resets for all interfaces except for the DMZ interface:

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

The following example enables resets for connections that terminate on the outside interface:

```
hostname(config)# service resetoutside
```

Related Commands

Command	Description
show running-config service	Displays the service configuration.

service (ctl-provider)

To specify the port to which the Certificate Trust List provider listens, use the **service** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

service port *listening_port*

no service port *listening_port*

Syntax Description

port *listening_port*	Specifies the certificate to be exported to the client.

Defaults

Default port is 2444.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **service** command in CTL provider configuration mode to specify the port to which the CTL provider listens. The port must be the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default port is 2444.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.

Commands	Description
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

service password-recovery

To enable password recovery, use the **service password-recovery** command in global configuration mode. To disable password recovery, use the **no** form of this command. Password recovery is enabled by default, but you might want to disable it to ensure that unauthorized users cannot use the password recovery mechanism to compromise the security appliance.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

Password recovery is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

On the ASA 5500 series adaptive security appliance, if you forget the passwords, you can boot the security appliance into ROMMON by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then set the security appliance to ignore the startup configuration by changing the configuration register (see the **config-register** command). For example if your configuration register is the default 0x1, then change the value to 0x41 by entering the **confreg 0x41** command. After reloading the security appliance, it loads a default configuration, and you can enter privileged EXEC mode using the default passwords. Then load the startup configuration by copying it to the running configuration and reset the passwords. Finally, set the security appliance to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the PIX 500 series security appliance, boot the security appliance into monitor mode by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then download the PIX password tool to the security appliance, which erases all passwords and **aaa authentication** commands.

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the security appliance prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the security appliance is configured to ignore the startup configuration at startup (in preparation for password recovery), then the security appliance changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the security appliance reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Examples

The following example disables password recovery for the ASA 5500 series adaptive security appliance:

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

The following example disables password recovery for the PIX 500 series security appliance:

```
hostname(config)# no service password-recovery
WARNING: Saving "no service password-recovery" in the startup-config will disable password
recovery via the npdisk application.  The only means of recovering from lost or forgotten
passwords will be for npdisk to erase all file systems including configuration files and
images.  You should make a backup of your configuration and have a mechanism to restore
images from the Monitor Mode command line.
```

The following example for the ASA 5500 series adaptive security appliance shows when to enter ROMMON at startup and how to complete a password recovery operation.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...
```

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
config-register	Sets the security appliance to ignore the startup configuration when it reloads.
enable password	Sets the enable password.
password	Sets the login password.

service-policy (class)

To apply a hierarchical policy map under another policy map, use the **service-policy** command in class configuration mode. To disable the service policy, use the **no** form of this command. Hierarchical policies are supported only for QoS traffic shaping when you want to perform priority queueing on a subset of shaped traffic.

service-policy *policymap_name*

no service-policy *policymap_name*

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map that includes the **priority** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used (the **priority-queue** command).

For hierarchical priority-queueing, perform the following tasks using Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.

c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.

4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

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

Related Commands

Command	Description
class (policy-map)	Identifies a class map for a policy map.
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
policy-map	Identifies actions to perform on class maps.
priority	Enables priority queueing.
service-policy (global)	Applies a policy map to an interface.
shape	Enables traffic shaping.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

service-policy (global)

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in global configuration mode. To disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.

service-policy *policymap_name* [**global** | **interface** *intf*]

no service-policy *policymap_name* [**global** | **interface** *intf*]

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map, and not an inspection policy map (**policy-map type inspect**).
global	Applies the policy map to all interfaces.
interface *intf*	Applies the policy map to a specific interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To enable the service policy, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features*—For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more details about the commands available for each feature.
3. **service-policy**—Assigns the policy map to an interface or globally.

Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with inspections, and an interface policy with TCP normalization, then both inspections and TCP normalization are applied to the interface. However, if you have a global policy with inspections, and an interface policy with inspections, then only the interface policy inspections are applied to that interface.

By default, the configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.

The default service policy includes the following command:

```
service-policy global_policy global
```

Examples

The following example shows how to enable the inbound_policy policy map on the outside interface:

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

The following commands disable the default global policy, and enables a new one called new_global_policy on all other security appliance interfaces:

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
service-policy (class)	Applies a hierarchical policy under another policy map.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

session

To establish a Telnet session to an intelligent SSM, such as an AIP SSM or a CSC SSM, use the **session** command in privileged EXEC mode.

session *slot* [**do** | **ip**]

Syntax Description

do	Executes a command on the SSM specified by the *slot* argument. Do not use the **do** keyword unless you are advised to do so by Cisco TAC.
ip	Configures logging IP addresses for the SSM specified by the *slot* argument. Do not use the **ip** keyword unless you are advised to do so by Cisco TAC.
slot	Specifies the SSM slot number, which is always 1.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **do** and **ip** keywords were added. These keywords are for use only when advised to do so by Cisco TAC.

Usage Guidelines

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

To end a session, enter **exit** or **Ctrl-Shift-6** then the **X** key.

Examples

The following example sessions to an SSM in slot 1:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Related Commands

Command	Description
debug session-command	Shows debug messages for sessions.

set connection

To specify connection limits within a policy map for a traffic class, use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous TCP and/or UDP connections, the connection limit is applied to each configured server separately. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one atack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.
random-sequence-number {**enable** | **disable**}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

Defaults

For the **conn-max**, **embryonic-conn-max**, **per-client-embryonic-max**, and **per-client-max** parameters, the default value of *n* is 0, which allows unlimited connections.

Sequence number randomization is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **per-client-embryonic-max** and **per-client-max** keywords were added.
8.0(2)	This command is now available for a Layer 3/4 management class map, for to-the-security appliance management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command (for through traffic) or **class-map type management** command (for management traffic). Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Note You can also configure maximum connections, maximum embryonic connections, and TCP sequence randomization in the NAT configuration. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

TCP Intercept Overview

Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the security appliance acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the security appliance receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

Disabling TCP Intercept for Management Packets for Clientless SSL Compatibility

By default, TCP management connections have TCP Intercept always enabled. When TCP Intercept is enabled, it intercepts the 3-way TCP connection establishment handshake packets and thus deprives the security appliance from processing the packets for clientless SSL. Clientless SSL requires the ability to process the 3-way handshake packets to provide selective ACK and other TCP options for clientless SSL connections. To disable TCP Intercept for management traffic, you can set the embryonic connection limit; only after the embryonic connection limit is reached is TCP Intercept enabled.

TCP Sequence Randomization Overview

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predecting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.

Examples

The following is an example of the use of the **set connection** command configure the maximum number of simultaneous connections as 256 and to disable TCP sequence number randomization:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

The following is an example of the use of the **set connection** command in a service policy that diverts traffic to a CSC SSM. The **set connection** command restricts each client whose traffic the CSC SSM scans to a maximum of five connections.

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

You can enter this command with multiple parameters or you can enter each parameter as a separate command. The security appliance combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

the output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection conn-max 600 embryonic-conn-max 50
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Removes all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy-map configurations.
show service-policy	Displays service policy configuration. Use the **set connection** keyword to view policies that include the **set connection** command.

set connection advanced-options

To specify advanced TCP connection options within a policy-map for a traffic class, use the **set connection advanced-options** command in class mode. To remove advanced TCP connection options for a traffic class within a policy map, use the **no** form of this command.

set connection advanced-options *tcp-mapname*

no set connection advanced-options *tcp-mapname*

Syntax Description

tcp-mapname	Name of a TCP map in which advanced TCP connection options are configured.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have configured the **policy-map** command and the **class** command, as well as the TCP map name, before issuing this command. See the description of the **tcp-map** command for detailed information.

Examples

The following example shows the use of the **set connection advanced-options** command to specify the use of a TCP map named localmap:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
class-map	Configures a traffic class by issuing at most one (with the exception of tunnel-group and default-inspection-traffic) match command, specifying match criteria, in the class-map mode.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

set connection decrement-ttl

To decrement the time to live value within a policy map for a traffic class, use the **set connection decrement-ttl** command in class configuration mode. To not decrement the time to live, use the **no** form of this command.

set connection decrement-ttl

no set connection decrement-ttl

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the security appliance does not decrement the time to live.

Command Modes

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

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

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

This command, along with the **icmp unreachable** command, is required to allow a traceroute through the security appliance that shows the security appliance as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

Related Commands

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

icmp unreachable	Controls the rate at which ICMP unreachables are allowed through the security appliance.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Displays service policy configuration.

set connection timeout

To specify connection timeouts within a policy map for a traffic class, use the **set connection timeout** command in class configuration mode. To remove the timeout, use the **no** form of this command.

set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh*:*mm*:*ss*] [**tcp** *hh*:*mm*:*ss* [**reset**]] [**half-closed** *hh*:*mm*:*ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

Syntax Description

dcd	Enables dead connection detection (DCD). DCD detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist. After a TCP connection times out, the security appliance sends DCD probes to the end hosts to determine the validity of the connection. If one of the end hosts fails to respond after the maximum retries are exhausted, the security appliance frees the connection. If both end hosts respond that the connection is valid, the security appliance updates the activity timeout to the current time and reschedules the idle timeout accordingly.
embryonic *hh*:*mm*:*ss*	Sets the timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:0:0. The default is 0:0:30. You can also set the value to 0, which means the connection never times out. A TCP connection for which a three-way handshake is not complete is an embryonic connection.
half-closed *hh*:*mm*:*ss*	Sets the idle timeout period until a half-closed connection is closed, between 0:5:0 and 1193:0:0. The default is 0:10:0. You can also set the value to 0, which means the connection never times out. Half-closed connections are not affected by DCD. Also, the security appliance does not send a reset when taking down half-closed connections.
max_retries	Sets the number of consecutive failed retries for DCD before declaring the connection as dead. The minimum value is 1 and the maximum value is 255. The default is 5.
reset	Sends a TCP RST packet to both end systems after TCP idle connections are removed.
retry_interval	Time duration in *hh*:*mm*:*ss* format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15.
tcp *hh*:*mm*:*ss*	Sets the idle timeout period after which an established connection closes.

Defaults

The default **embryonic** timeout is 30 seconds.

The default **half-closed** idle timeout is 10 minutes.

The default **dcd** *max_retries* value is 5.

The default **dcd** *retry_interval* value is 15 seconds.

The default **tcp** idle timeout is 1 hour.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Support for DCD was added.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command. Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection timeout** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Cisco ASA 5500 Series Configuration Guide using the CLI*.

Enabling DCD changes the behavior of idle-timeout handling in the TCP normalizer. DCD probing resets the idle timeout on the connections seen in the **show conn** command. To determine when a connection that has exceeded the configured timeout value in the timeout command but is kept alive due to DCD probing, the **show service-policy** command includes counters to show the amount of activity from DCD.

Examples

The following example sets the connection timeouts for all traffic:

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection timeout tcp 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

You can enter **set connection** commands with multiple parameters or you can enter each parameter as a separate command. The security appliance combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection timeout embryonic 0:40:0
```

the output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.

clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configure connection values.
show running-config policy-map	Display all current policy-map configurations.
show service-policy	Displays counters for DCD `and` other service activity.

set metric

To set the metric value for a routing protocol, use the **set metric** command in route-map configuration mode. To return to the default metric value, use the **no** form of this command.

set metric *value*

no set metric *value*

Syntax Description

value	Metric value.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **no set metric** *value* command allows you to return to the default metric value. In this context, the *value* is an integer from 0 to 4294967295.

Examples

The following example shows how to configure a route map for OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

set metric-type

To specify the type of OSPF metric routes, use the **set metric-type** command in route-map configuration mode. To return to the default setting, use the **no** form of this command.

```
set metric-type {type-1 | type-2}

no set metric-type
```

Syntax Description

type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.

Defaults

The default is **type-2**.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example shows how to configure a route map for OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# set metric-type type-2
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

setup

To configure a minimal configuration for the security appliance using interactive prompts, enter the **setup** command in global configuration mode. This configuration provides connectivity to use ASDM. See also the **configure factory-default** command to restore the default configuration.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The setup dialog automatically appears at boot time if there is no startup configuration in Flash memory.

Before you can use the **setup** command, you must have an inside interface already configured. The PIX 500 series default configuration includes an inside interface (Ethernet 1), but the ASA 550 series default configuration does not. Before using the **setup** command, enter the **interface** command for the interface you want to make inside, and then the **nameif inside** command.

In multiple context mode, you can use the **setup** command in the system execution space and for each context.

When you enter the **setup** command, you are asked for the information in Table 24-1. The system **setup** command includes a subset of these prompts. If there is already a configuration for the prompted parameter, it appears in barckets so you can either accept it as the default or override it by entering something new.

Table 24-1 Setup Prompts

Prompt	Description
`Pre-configure Firewall now through interactive prompts [yes]?`	Enter **yes** or **no**. If you enter **yes**, the setup dialog continues. If **no**, the setup dialog stops and the global configuration prompt (`hostname(config)#`) appears.

Table 24-1 Setup Prompts (continued)

`Firewall Mode [Routed]:`	Enter **routed** or **transparent**.
`Enable password:`	Enter an enable password. (The password must have at least three characters.)
`Allow password recovery [yes]?`	Enter **yes** or **no**.
`Clock (UTC):`	You cannot enter anything in this field. UTC time is used by default.
`Year:`	Enter the year using four digits, for example, 2005. The year range is 1993 to 2035.
`Month:`	Enter the month using the first three characters of the month; for example, **Sep** for September.
`Day:`	Enter the day of the month, from 1 to 31.
`Time:`	Enter the hour, minutes, and seconds in 24-hour time format. For example, enter **20:54:44** for 8:54 p.m and 44 seconds.
`Inside IP address:`	Enter the IP address for the inside interface.
`Inside network mask:`	Enter the network mask that applies to the inside IP address. You must specify a valid network mask, such as 255.0.0.0 or 255.255.0.0.
`Host name:`	Enter the hostname that you want to display in the command line prompt.
`Domain name:`	Enter the domain name of the network on which the security appliance runs.
`IP address of host running Device Manager:`	Enter the IP address of the host that needs to access ASDM.
`Use this configuration and write to flash?`	Enter **yes** or **no**. If you enter **yes**, the inside interface is enabled and the requested configuration is written to the Flash partition. If you enter **no**, the setup dialog repeats, beginning with the first question: `Pre-configure Firewall now through interactive prompts [yes]?` Enter **no** to exit the setup dialog or **yes** to repeat it.

Examples

This example shows how to complete the **setup** command prompts:

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
```

```
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

Related Commands

Command	Description
configure factory-default	Restores the default configuration.

shape

To enable QoS traffic shaping, use the **shape** command in class configuration mode. If you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate, called *traffic shaping*. To remove this configuration, use the **no** form of this command.

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

Syntax Description

average *rate*	Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000. See the "Usage Guidelines" section for more information about how the time period is calculated.
burst_size	Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Defaults

If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Command Modes

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

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

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable traffic shaping, use the Modular Policy Framework:

1. **policy-map**—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.

   b. **shape**—Apply traffic shaping to the class map.
   c. (Optional) **service-policy**—Call a different policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.
2. **service-policy**—Assigns the policy map to an interface or globally.

Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPSec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the burst size value. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information about the token bucket.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queueing, see the **priority** command):
  - The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
  - When the queue limit is reached, packets are tail-dropped.
  - Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
  - The time interval is derived by *time_interval* = *burst_size* / *average_rate*. The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

    Average Rate = 1000000

    Burst Size = 1000000

    In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

How QoS Features Interact

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

See the following supported feature combinations per interface:

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

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

You cannot configure traffic shaping and standard priority queueing for the same interface; only hierarchical priority queueing is allowed. For example, if you configure standard priority queueing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

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

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

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

Related Commands

Command	Description
class	Identifies the class map on which you want to perform actions in a policy map.
police	Enables QoS policing.
policy-map	Identifies actions to apply to traffic in a service policy.
priority	Enables QoS priority queueing.
service-policy (class)	Applies a hierarchical policy map.
service-policy (global)	Applies a service policy to interface(s).
show service-policy	Shows QoS statistics.

show aaa local user

To show the list of usernames that are currently locked, or to show details about the username, use the show **aaa local user** command in global configuration mode.

show aaa local user [**locked**]

Syntax Description

locked	(Optional) Shows the list of usernames that are currently locked.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you omit the optional keyword **locked**, the security appliance displays the failed-attempts and lockout status details for all AAA local users.

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Examples

The following example shows use of the **show aaa local user** command to display the lockout status of all usernames:

This example shows the use of the **show aaa local user** command to display the number of failed authentication attempts and lockout status details for all AAA local users, after the limit has been set to 5:

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                 6       Y       test
    -                 2       N       mona
    -                 1       N       cisco
    -                 4       N       newuser
hostname(config)#
```

This example shows the use of the **show aaa local user** command with the **lockout** keyword to display the number of failed authentication attempts and lockout status details only for any locked-out AAA local users, after the limit has been set to 5:

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                6       Y       test
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures the maximum number of times a user can enter a wrong password before being locked out.
clear aaa local user fail-attempts	Resets the number of failed attempts to 0 without modifying the lockout status.
clear aaa local user lockout	Clears th e lockout status of the specified user or all users and sets their failed attempts counters to 0.

show aaa-server

To display AAA server statistics for AAA servers, use the **show aaa-server** command in privileged EXEC mode.

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Shows statistics for the LOCAL user database.
groupname	(Optional) Shows statistics for servers in a group.
host *hostname*	(Optional) Shows statistics for a particular server in the group.
protocol *protocol*	(Optional) Shows statistics for servers of the specified protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

By default, all AAA server statistics display.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	The http-form protocol was added.
8.0(2)	The server status now shows if the status was changed manually using the **aaa-server active** or **fail** command.

Examples

This example shows the use of the **show aaa-server** command to display statistics for a particular host in server group group1:

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
```

```
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

Field descriptions for the **show aaa-server** command are shown below:

Field	Description
Server Group	The server group name specified by the **aaa-server** command.
Server Protocol	The server protocol for the server group specified by the **aaa-server** command.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the security appliance and the AAA server. You can specify the RADIUS authentication port using the **authentication-port** command. You can specify the RADIUS accounting port using the **accounting-port** command. For non-RADIUS servers, the port is set by the **server-port** command.

Server status	The status of the server. You see one of the following values:
	• ACTIVE—The security appliance will communicate with this AAA server.
	• FAILED—The security appliance cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated.
	If the status is followed by "(admin initiated)," then the server was manually failed or reactivated using the **aaa-server active** or **fail** command.
	You also see the date and time of the last transaction in the following form:
	`Last transaction ({success | failure}) at time timezone date`
	If the security appliance has never communicated with the server, the message shows as the following:
	`Last transaction at Unknown`

Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.

Field	Description
Number of authentication requests	The number of authentication requests sent by the security appliance. This value does not include retransmissions after a timeout.
Number of authorization requests	The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic (for TACACS+ servers), or for WebVPN and IPSec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout
Number of accounting requests	The number of accounting requests. This value does not include retransmissions after a timeout
Number of retransmissions	The number of times a message was retransmitted after an internal timeout. This value applies only to Kerberos and RADIUS servers (UDP)
Number of accepts	The number of successful authentication requests.
Number of rejects	The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.
Number of challenges	The number of times the AAA server required additional information from the user after receiving the initial username and password information.
Number of malformed responses	N/A. Reserved for future use.
Number of bad authenticators	The number of times that one of the following occurs: • The “authenticator” string in the RADIUS packet is corrupted (rare). • The shared secret key on the security appliance does not match the one on the RADIUS server. To fix this problem, enter the proper server key. This value only applies to RADIUS.
Number of timeouts	The number of times the security appliance has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.
Number of unrecognized responses	The number of times that the security appliance received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server got corrupted, which is rare.

Related Commands

Command	Description
show running-config aaa-server	Display statistics for all servers in the indicated server group or for a particular server.
clear aaa-server statistics	Clear the AAA server statistics.

show access-list

To display the counters for an access list, use the **show access-list** command in privileged EXEC mode.

show access-list *id_1* [...[*id_2*]] [**brief**]

Syntax Description

acl_name_ 1	A name or set of characters that identifies an existing access list.
acl_name_2	A name or set of characters that identifies an existing access list.
brief	Displays the access list identifiers and hit count in hexadecimal format.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	Support for the **brief** keyword was introduced.

Usage Guidelines

You can display multiple access lists at one time by entering the access list identifiers in one command.

You can specify the **brief** keyword to display access list hit count and identifiers information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in two columns, and are the same identifiers used in syslog 106023 and 106100.

Examples

The following is sample output from the **show access-list** command:

```
hostname# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list 101; 10 elements
access-list 101 line 1 extended permit tcp any eq www any (hitcnt=0) 0xa14fc533
access-list 101 line 2 extended permit tcp any eq www any eq www (hitcnt=0) 0xaa73834e
access-list 101 line 3 extended permit tcp any eq www any range telnet www (hitcnt=0)
0x49ac02e6
access-list 101 line 4 extended permit tcp any range telnet www any range telnet www
(hitcnt=0) 0xa0021a9f
access-list 101 line 5 extended permit udp any range biff www any (hitcnt=0) 0xf89a7328
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43 access-list
101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
```

```
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

The output contains a unique hexamdecimal identifier for each access control entry at the end of each line.

The following is sample output from the **show access-list brief** command:

```
hostname (config)# sh access-list abc brief

abc:
28676dfa 00000000 00000001
bbec063f f0109e02 000000a1
3afd0576 f0109e02 000000c2
a83ddc02 f0109e02 00000021
hostname (config)#
```

The first two columns display identifiers in hexadecimal format, and the third column lists the hit count in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. If the hit count is zero, no information is displayed.

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show running-config access-list	Displays the current running access-list configuration.

show activation-key

To display the running activation key and licensed features in the configuration that are enabled by your activation key, including the number of contexts allowed, use the **show activation-key** command in privileged EXEC mode.

show activation-key [detail]

Note This command is not supported on the PIX platform.

Syntax Description

The **detail** keyword displays the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	The **detail** keyword was added.

Usage Guidelines

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the security appliance flash file system is the same as the activation key running on the security appliance, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the security appliance flash file system is different from the activation key running on the security appliance, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If you downgrade your activation key, the display shows that the running key (the old key) differs from the key that is stored in the Flash (the new key). When you restart, the security appliance uses the new key.

- If you upgrade your key to enable extra features, the new key starts running immediately without a restart.
- For the PIX Firewall platform, if there is any change in the failover feature (R/UR/FO) between the new key and the old key, it prompts for confirmation. If the user enters **n**, it aborts the change; otherwise it updates the key in the Flash file system. When you restart the security appliance uses the new key.
- If you downgrade to an earlier release, your key for the current release might allow for more security contexts than the earlier release supports. When the value of the security contexts in the key exceeds the platform limit, the following message appears in the show activation-key output:

```
The Running Activation Key feature: 50 security contexts exceeds the limit in the
platform, reduce to 20 security contexts.
```

- If you downgrade to an earlier release, your key for the current release might enable GTP/GPRS even though it is not allowed in the earlier release. When the key enables GTP/GPRS but the software version does not allow it, the following message appears in the show activation-key output:

```
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
GTP/GPRS.
```

A temporary activation key is a time-based activation key, which you activate or deactivate using the **activation-key** command. When you deactivate a temporary activation key, you may assign a permanent activation key. A permanent activation key is a nontime-based activation key. You cannot delete temporary activation keys, because you can reactivate them at a later date.

Both temporary and permanent activation keys are stored on the flash file system. The running activation key is the one being applied. You may apply only one temporary activation key at a time. If you apply a temporary activation key on a security appliance that already has a temporary activation key, the old temporary activation key is deactivated and the new temporary activation key is applied.

The security appliance tracks all temporary activation keys that have been activated. When a temporary activation key expires, the security appliance notifies you of the expiration. After the temporary activation key expires, it can no longer appear. Non-active temporary activation keys are keys that have been applied and then overwritten by another temporary or permanent activation key.

Examples

This example shows how to display the commands in the configuration for features that are enabled by your activation key:

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada
The Running Activation Key feature: 50 security contexts exceeds the limit in the
platform, reduce to 20 security contexts.
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable
GTP/GPRS.

License Features for this Platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 50
Inside Hosts                : Unlimited
Failover                    : Enabled
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL-filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
```

```
VPN Peers                    : 5000
Advanced Endpoint Assessment: Disabled
UC Proxy Sessions            : 2

The flash activation key is the SAME as the running key.
```

This example shows how to display the licensed features in the configuration that are enabled by temporary and permanent activation keys:

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
Permanent Flash Activation Key: 0x31245147 0x3834b49a 0x98b391b4
0x95b83030 0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 50
GTP/GPRS                     : Enabled
VPN Peers                    : 5000
WebVPN Peers                 : 5000
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions            : 2

Temporary Flash Activation Key: 0x051e96ff 0x98937617 0x79cbe717
0x502449e7 0x862b92ab

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Disabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
WebVPN Peers                 : 2
AnyConnect for Mobile        : Enabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions            : 2
This is a time-based license that will expire in 27 day(s).
```

This example shows how to display the licensed features in the configuration that are enabled by a permanent activation key:

```
hostname(config)# show activation-key detail
Serial Number:  JMX0916L0Z4
No active temporary key.
Running Activation Key: 0x31245147 0x3834b49a 0x98b391b4 0x95b83030
0xc13cf897

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
```

```
VPN-DES                       : Enabled
VPN-3DES-AES                  : Enabled
Security Contexts             : 50
GTP/GPRS                      : Enabled
VPN Peers                     : 5000
WebVPN Peers                  : 5000
AnyConnect for Mobile         : Enabled
AnyConnect for Linksys phone : Enabled
Advanced Endpoint Assessment : Enabled
UC Proxy Sessions             : 2

This platform has an ASA 5540 VPN Premium license.

The flash activation key is the SAME as the running key.

Non-active temporary keys:                              Time left
-----------------------------------------------------------------
0x2a53d6   0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2  28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397  27 day(s
```

Related Commands

Command	Description
activation-key	Changes the activation key.

show ad-groups

To display groups that are listed on an Active Directory server, use the **show ad-groups** command in privileged EXEC mode:

show ad-groups *name* [**filter** *string*]

Syntax Description

name	The name of the Active Directory server group to query.
string	A string within quotes specifying all or part of the group name to search for.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **show ad-groups** command applies only to Active Directory servers that use the LDAP protocol to retrieve groups. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

When the LDAP attribute type = LDAP, the default time that the security appliance waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.

Note If the Active Directory server has a large number of groups, the output of the **show ad-groups** command may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

Examples

```
hostname# show ad-groups LDAP-AD17
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     46
Account Operators
Administrators
APP-SSL-VPN CIO Users
Backup Operators
Cert Publishers
CERTSVC_DCOM_ACCESS
Cisco-Eng
DHCP Administrators
DHCP Users
Distributed COM Users
DnsAdmins
DnsUpdateProxy
Doctors
Domain Admins
Domain Computers
Domain Controllers
Domain Guests
Domain Users
Employees
Engineering
Engineering1
Engineering2
Enterprise Admins
Group Policy Creator Owners
Guests
HelpServicesGroup
```

The next example shows the same command with the **filter** option:

```
hostname(config)# show ad-groups LDAP-AD17 filter “Eng”
.
Server Group   LDAP-AD17
Group list retrieved successfully
Number of Active Directory Groups     4
Cisco-Eng
Engineering
Engineering1
Engineering2
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
group-search-timeout	Adjusts the time the security appliance waits for a response from an Active Directory server for a list of groups.

show admin-context

To display the context name currently assigned as the admin context, use the **show admin-context** command in privileged EXEC mode.

show admin-context

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show admin-context** command. The following example shows the admin context called "admin" and stored in the root directory of flash:

```
hostname# show admin-context
Admin: admin flash:/admin.cfg
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
clear configure context	Removes all contexts.
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

show arp

To view the ARP table, use the **show arp** command in privileged EXEC mode.

show arp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	Added dynamic ARP age to the display.

Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state “alias.”

Examples

The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
hostname# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp-inspection

To view the ARP inspection setting for each interface, use the **show arp-inspection** command in privileged EXEC mode.

show arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output from the **show arp-inspection** command:

```
hostname# show arp-inspection
interface                 arp-inspection         miss
----------------------------------------------------
inside1                   enabled                flood
outside                   disabled                -
```

The **miss** column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp statistics

To view ARP statistics, use the show arp statistics command in privileged EXEC mode.

show arp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show arp statistics** command:

```
hostname# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

Table 2 shows each field description.

Table 24-2 show arp statistics Fields

Field	Description
Number of ARP entries	The total number of ARP table entries.
Dropped blocks in ARP	The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.
Maximum queued blocks	The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.

Table 24-2 show arp statistics Fields (continued)

Field	Description
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all security appliance interfaces that were from the same IP address as that of a security appliance interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the security appliance as part of the ARP-Defense mechanism.
Total ARP retries	The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.
Unresolved hosts	The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.
Maximum unresolved hosts	The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the security appliance booted up.

Related Commands

Command	Description
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics and resets the values to zero.
show arp	Shows the ARP table.
show running-config arp	Shows the current configuration of the ARP timeout.

show asdm history

To display the contents of the ASDM history buffer, use the **show asdm history** command in privileged EXEC mode.

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

Syntax Description

asdmclient	(Optional) Displays the ASDM history data formatted for the ASDM client.
feature *feature*	(Optional) Limits the history display to the specified feature. The following are valid values for the *feature* argument: • **all**—Displays the history for all features (default). • **blocks**—Displays the history for the system buffers. • **cpu**—Displays the history for CPU usage. • **failover**—Displays the history for failover. • **ids**—Displays the history for IDS. • **interface** *if_name*—Displays the history for the specified interface. The *if_name* argument is the name of the interface as specified by the **nameif** command. • **memory**—Displays memory usage history. • **perfmon**—Displays performance history. • **sas**—Displays the history for Security Associations. • **tunnels**—Displays the history for tunnels. • **xlates**—Displays translation slot history.
snapshot	(Optional) Displays only the last ASDM history data point.
view *timeframe*	(Optional) Limits the history display to the specified time period. Valid values for the *timeframe* argument are: • **all**—all contents in the history buffer (default). • **12h**—12 hours • **5d**—5 days • **60m**—60 minutes • **10m**—10 minutes

Defaults

If no arguments or keywords are specified, all history information for all features is displayed.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm history** command to the **show asdm history** command.

Usage Guidelines

The **show asdm history** command displays the contents of the ASDM history buffer. Before you can view ASDM history information, you must enable ASDM history tracking using the **asdm history enable** command.

Examples

The following is sample output from the **show asdm history** command. It limits the output to data for the outside interface collected during the last 10 minutes.

```
hostname# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

The following is sample output from the **show asdm history** command. Like the previous example, it limits the output to data for the outside interface collected during the last 10 minutes. However, in this example the output is formatted for the ASDM client.

```
hostname# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|6
2469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|6
2553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|6
2636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|6
2723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|2
5026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|2
5102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|2
5169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|2
5381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750
|750|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|751|751|7
51|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|752|753|753|753|753
|753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|55|5
5|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|5
5|55|55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|4
381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|5
401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698
|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349
|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|33
49|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|5
|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|7|
6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|3750
10|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|375373|375
395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|375738|375761|37
5794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115|376147|376168|3
76200|376224|376253|376289|376315|376365|376400|376436|376463|376508|376530|376553|376583|
376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|1
28|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
hostname#
```

The following is sample output from the **show asdm history** command using the **snapshot** keyword:

```
hostname# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
```

```
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
```

```
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
```

```
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
hostname#
```

Related Commands

Command	Description
asdm history enable	Enables ASDM history tracking.

show asdm image

To the current ASDM software image file, use the show **asdm image** command in privileged EXEC mode.

show asdm image

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm image** command to the **show asdm image** command.

Examples

The following is sample output from the **show asdm image** command:

```
hostname# show asdm image

Device Manager image file, flash:/ASDM
```

Related Commands

Command	Description
asdm image	Specifies the current ASDM image file.

show asdm log_sessions

To display a list of active ASDM logging sessions and their associated session IDs, use the **show asdm log_sessions** command in privileged EXEC mode.

show asdm log_sessions

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the security appliance. Each ASDM logging session is assigned a unique session ID. You can use this session ID with the **asdm disconnect log_session** command to terminate the specified session.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

Examples

The following is sample output from the **show asdm log_sessions** command:

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect log_session	Terminates an active ASDM logging session.

show asdm sessions

To display a list of active ASDM sessions and their associated session IDs, use the **show asdm sessions** command in privileged EXEC mode.

show asdm sessions

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm sessions** command to the **show asdm sessions** command.

Usage Guidelines

Each active ASDM session is assigned a unique session ID. You can use this session ID with the **asdm disconnect** command to terminate the specified session.

Examples

The following is sample output from the **show asdm sessions** command:

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect	Terminates an active ASDM session.